

Personvernerklæringer

Virksomheters informasjon om behandlingen av personopplysninger gjennom internett

Kandidatnummer: 752

Leveringsfrist: 25.4.2013

Antall ord: 17.910



Innholdsfortegnelse

1	INNLEDNING	1
1.1	Oppgavens tema	1
1.2	Presentasjon av problemstilling	2
2	NÆRMERE OM UNDERSØKELSESOPPLEGGET.....	3
2.1	Valg av undersøkelsesområde og utvalg av erklæringer	3
2.2	Gjennomgang av undersøkelsesopplegget.....	4
2.3	Rettskilder og juridisk metode.....	8
2.3.1	Lovgivning og EU-direktiv	8
2.3.2	Praksis	12
2.3.3	Internasjonale rettskilder	13
2.3.4	Særskilt juridisk litteratur, bransjeorganer og rådgivning.....	14
3	DEN RETTSLIGE BEGRUNNELSEN FOR BRUKEN AV PERSONVERNERKLÆRINGER	15
3.1	Hva er en personvernerklæring?.....	15
3.2	Forholdet til aktuell lovgivning	17
3.3	Den videre rettstilstanden	22
4	EN EMPIRISK UNDERSØKELSE AV INNHOLDET I PERSONVERNERKLÆRINGENE TIL IF OG STOREBRAND.....	27
4.1	Innledning, tilgjengeligheten til erklæringene.....	27
4.2	Informasjon om selskapene	28
4.3	Hvordan selskapene kommuniserer	29
4.3.1	Innsamlingen av personopplysninger.....	29
4.3.2	Webanalyseverktøy og bruken av informasjonskapsler.....	30
4.3.3	Mottakeren av informasjonen	35

4.4	Informasjon om selskapenes behandling av personopplysninger.....	36
4.4.1	Hvilke opplysninger samles inn	36
4.4.2	Formålet med behandlingen	37
4.4.3	Utlevering.....	40
4.4.4	Frivillighet.....	43
4.5	Informasjon om rettigheter	45
4.5.1	Lagring, sletting og retting	45
4.5.2	Innsynsrett	47
4.5.3	Andre rettigheter	48
4.6	Andre forhold som er tatt med i erklæringen	49
4.6.1	Ansvar	49
4.6.2	Immaterialrett og markedsføringsrett.....	50
5	I HVILKEN GRAD ER PERSONVERNERKLÆRINGER HENSIKTSMESSIGE?.....	52
5.1	Gis brukerne og kundene til If og Storebrand hensiktsmessig informasjon i erklæringene?.....	52
5.1.1	Premiss for vurderingen	52
5.1.2	Informasjonsplikten vurdert opp mot innholdet i erklæringene.....	53
5.1.3	Konklusjon	57
5.2	Generelle betraktninger og utfordringer ved personvernerklæringer	59
5.2.1	Informasjonen som gis	59
5.2.2	Tidspunkt for informasjonen.....	60
5.2.3	Ulike brukere krever ulik informasjon.....	61
5.2.4	Er loven tilpasset nyere teknologi?	63
5.2.5	Lovfesting	64
5.2.6	Erklæringene må leses.....	65
6	KILDER	68
6.1	Lover.....	68
6.2	Forskrifter	68

6.3	Forarbeider.....	69
6.4	Rettsavgjørelser	69
6.5	Direktiver.....	69
6.6	Avgjørelser av Personvernemnda	70
6.7	Uttalelser fra Artikkel 29-gruppen	70
6.8	Bøker	72
6.9	Nettdokumenter	72
6.10	Nettsider til de mest brukte kilder	76
7	VEDLEGG	76

1 Innledning

1.1 Oppgavens tema

En virksomhet som utøver aktivitet gjennom internett vil kunne oppleve utfordringer ved etterlevelsen av personvernlovgivningen. For en virksomhet vil personverninteresser skape utfordringer allerede ved opprettelsen av et nettsted, gjennom blant annet krav til sikker behandling av personopplysninger, lovpålagt informasjon til kunder og oversikt over behandlingen som forekommer, jfr. personopplysningsloven¹. En nettside vil ha mange ulike besøkende, som søker informasjon om ulike forhold ved virksomheten. Gjennom normen om innebygget personvern anbefales alle virksomheter blant annet å vise åpenhet om hvordan personvernet blir ivaretatt,² og en utfordring vil være hvordan dette best kan gjøres.

På den andre siden av personvernet står brukerne av internett, og deres opplevelse av et personopplysningsvern ved bevegelse på nettet. Det kan være vanskelig for en alminnelig bruker av en nettside å holde oversikt over de opplysninger en gir ut om seg selv til virksomheter, og man vil sjeldent ha full oversikt over de spor en legger igjen. Som en del av en virksomhets etterlevelse av personvernlovgivningen fremstår teksten på en nettside om informasjon om behandling av personopplysninger, ofte kalt personvernerklæringer, som et redskap for dette. Hva en personvernerklæring faktisk er, er uklart. Det foreligger ingen legaldefinisjon av hva et slikt dokument er, og det forekommer heller ikke alltid under navnet "*personvernerklæring*". Utgangspunktet for oppgaven vil være å stille spørsmål om hva en slik erklæring *kan* bidra med. Det er uklart hva en personvernerklæring bidrar med med tanke på oppfyllelsen av lovgivningen, hva den bør inneholde, og om brukerne av internett får tilstrekkelig informasjon til å ivareta sitt eget personvern gjennom en slik. Dette vil være tema for oppgaven.

¹ Lov om behandling av personopplysninger (personopplysningsloven(pol.)) av 14. april 2000 nr. 31

² International Conference of Data Protection and Privacy Commissioners(2010) og Datatilsynet(2013 d)

1.2 Presentasjon av problemstilling

Den overordnede problemstillingen er hvilket bidrag personvernerklæringer gir i oppfyllelsen av personvernlovgivningen. Dette søker jeg svar på gjennom tre spørsmål.

Det første spørsmålet er

- Hva er den rettslige begrunnelsen for bruken av personvernerklæringer?

Personopplysningsloven har ingen hjemmel for bruken av personvernerklæringer, men likevel brukes slike erklæringer i stor utstrekning. Det vil være interessant å sammenstille de ulike rettslige grunnlag og anbefalinger om erklæringer som foreligger, for å se hvilke regler i personvernlovgivningen som søkes oppfylt.

Det andre spørsmålet er

- Hvilket personvernrettslig innhold har personvernerklæringene til If og Storebrand?

Med dette spørsmålet søker jeg svar på om og på hvilken måte Storebrand og If oppfyller personvernlovgivningen gjennom sine personvernerklæringer. Jeg vil foreta en undersøkelse av de to erklæringene, der innholdet sammenholdes med gjeldende krav som oppstilles i personvernlovgivningen. Oppgavens innhold vil derfor i stor grad defineres av innholdet i de utvalgte erklæringene.

Det tredje spørsmålet er

- Kan personvernerklæringer sies å være hensiktsmessige for å ivareta reglene om innsyn, informasjon og rettigheter i forbindelse med behandling av personopplysninger på internett?

Med dette spørsmålet søker jeg svar på om en personvernerklæring kan gi tilstrekkelig informasjon til brukerne av et nettsted, og kundene av en virksomhet, og se på hvilke utfordringer som eksisterer i denne sammenheng.

2 Nærmere om undersøkelsesopplegget

2.1 Valg av undersøkelsesområde og utvalg av erklæringer

For å besvare oppgavens overordnede problemstilling vil jeg foreta en empirisk undersøkelse av to personvernerklæringer, hentet fra nettsidene til to forsikringsselskaper:

- www.if.no³
- www.storebrand.no⁴

Jeg har valgt å ta for meg personvernerklæringen til If Skadeforsikring NUF (heretter: If) og Storebrand ASA (heretter: Storebrand); begge er store forsikringsselskaper i det norske markedet, og begge har en slik erklæring liggende tilgjengelig for sine brukere på hjemmesiden.

I Meld. St. 11 (2012-2013) *Personvern – utsikter og utfordringer* nevnes forsikringsselskaper som et eksempel på en bransje hvor det finnes gode eksempler på personverninformasjon på nett.⁵ Å analysere virksomheter som har svært kortfattede og snevre erklæringer for sine brukere vil være lite lærerikt. Det er liten mulighet til prinsipielle drøftelser utover hva som burde vært med. Jeg har derfor valgt å ta for meg den bransjen som regnes som typisk god, fordi jeg antar at en her har mest å lære.

Ved å ta for meg erklæringer som antas å være grundige med tanke på personverninformasjon som gis, vil jeg også på et mer prinsipielt plan kunne drøfte slike erklæringer opp mot personvernlovgivningen. En nødvendig konsekvens av forsikringsvirksomhet er at det i stor utstrekning behandles personopplysninger som en del av virksomheten. If og Storebrand behandler derfor personopplysninger i stor grad, ikke kun som en del av nettaktivitet. Data-

³ Se vedlegg 1

⁴ Se vedlegg 2

⁵ Jfr. Meld. St.11 (2012-2013) side 64, 2.spalte

tilsynet foretok i en rapport av 27. juni 2011 kalt "*Fortell meg hva dere gjør!*"⁶ en analyse av en rekke virksomheters bruk av personvernerklæringer. If og Storebrand var en del av dette utvalget, og rapporten vil være et bakteppe for en videre analyse av deres publiserte erklæringer.

2.2 Gjennomgang av undersøkelsesopplegget

Jeg vil i det videre først redegjøre kort for de rettskilder som generelt gjør seg gjeldende innen personvernområdet. Jeg vil gjennomgå aktuell lovgivning og andre særlig aktuelle rettskilder, med tanke på utvalget av erklæringer som senere skal analyseres.

Jeg vil deretter ta fatt på oppgavens første hoveddel, kapittel 3, hvor jeg redegjør for hva en personvernerklæring kan sies å være, og rettslige utgangspunkter for bruken av slike.

Jeg vil i oppgavens neste del, kapittel 4, foreta en konkret undersøkelse av innholdet i erklæringene til If og Storebrand. Jeg vil undersøke hva de enkelte erklæringer inneholder, og analysere dette opp mot gjeldende regelverk. Ulikheter mellom de to vil også drøftes.

De aktuelle erklæringer vil analyseres gjennom ett og ett tema, der innholdet avgjør de rettsspørsmål som drøftes. Metoden vil være å gjengi innholdet, trekke frem de relevante bestemmelser i lovgivningen, og deretter drøfte om og på hvilken måte Storebrand og If oppfyller personvernlovgivningen. Da det kun er to erklæringer jeg tar for meg, vil det ikke være en representativ redegjørelse av personvernerklæringer generelt. Men nettopp ved å knytte innholdet i erklæringene opp mot personvernlovgivningen vil oppgaven kunne belyse hvordan lovgivningen potensielt kan utøves i praksis utad; nettopp gjennom en personvernerklæring.

⁶ Datatilsynet(2011)

Personvernerklæringer både gjengir, presiserer og supplerer personopplysningsloven, og jeg vil derfor også berøre tilgrensende områder til personvern, slik som innsamlingen av elektroniske spor utenfor personopplysningslovens område. Oppgavens begrensede omfang tilsier at ikke alle deler ved de aktuelle personvernerklæringer vil kunne analyseres like inngående. For innhold som kan knyttes til lovgivning utover personvernets område vil jeg kun kort referere til rettsområdet. Jeg avgrenser dermed mot de markedsførings- og immateriellrettslige spørsmål som dukker opp.

De to utvalgte erklæringer har ved første øyekast tilnærmet samme innhold, presentert gjennom overskrifter som i stor grad ligner. Likevel er det noe ulikt innhold som presenteres, og inndelingen etter de enkelte temaer er lagt forskjellig opp. Det må være opp til meg å definere overordnede temaer, trekke ut informasjon fra de enkelte erklæringene og sette de opp mot hverandre, og deretter drøfte de delene jeg vurderer å være sammenlignbart.

I tabellen under presenteres overskriftene i erklæringene, holdt opp mot kapittelinndeling i oppgaven. Slik kan leseren av oppgaven få en forståelse for undersøkelsesmetoden. Som en ser av tabellen har ikke de ulike avsnitt i erklæringene alltid samme tittel for de samme drøftelser, og tabellen kan brukes for å finne igjen temaene i oppgaven i de aktuelle erklæringer.

Kapittel i oppgaven	Avsnittsoverskrift hos If ⁷	Avsnittsoverskrift hos Storebrand ⁸	Særlig relevant lovgivning
4.1 Innledning, tilgjengeligheten til erklæringene			WP 43
4.2 Informasjon om selskapene	Behandlingsansvarlig	Behandlingsansvarlig	Pol.§ 11 § 2nr.4 § 13 § 16 § 19(1) a
4.3 Hvordan selskapene kommuniserer	Opptak og lagring av kundekommunikasjon, Tilleggsdokumentet "cookies" ⁹	Innhenting av personopplysninger, Cookies og analyseverktøy	Pol.§ 13 § 11 Forslag ny § 2-7B i ekomloven Direktiv 2009/136/EF Pol.§ 19(1) e
4.4 Informasjon om selskapenes behandling	Helseopplysninger, Behandlingsansvarlig, Ifs behandling av personopplysninger	Innhenting av personopplysninger, Hva bruker Storebrand opplysningene til? Spesielt om markedsføring, Konsernsamtykke, Slik videreformidler vi personopplysninger	Pol.§ 20 § 15 § 8 § 11 § 21 §§29 og 30 § 19(1) b-d WP 153
4.5 Informasjon om rettigheter	Innhenting av personopplysninger, Innsyn og retting, Opptak og lagring av kundekommunikasjon, Oppbevaring og sletting	Personvernombud, Lagring av opplysninger, Dine rettigheter	Pol.§ 18 § 27 § 28 pof.§ 7-12 § 19(1) e
4.6 Andre forhold	Reservasjon	Ansvar ved feil, Mangler og tilgjengelighet, Immaterialrett, Lenker	Avtalelov åndsverkslov markedsføringslov pol.§ 46

⁷ Vedlegg 1, If(2013 a)

⁸ Vedlegg 2, Storebrand(2013 a)

⁹ Vedlegg 3, If(2013 b)

Selve dokumentet jeg skal ta for meg er en publisert tekst på en nettside, som kan leses av alle. Jeg må trekke ut informasjonen som står, og analysere dette. For å velge metode for analyse av teksten vil det være naturlig å sammenligne med andre skrevne tekster om juridiske forhold. Teksten har både en avgiver og en mottaker, noe som medfører at en slik erklæring ligner på en avtale. Likevel må erklæringen sees på som en ensidig tekst, og vil nok ikke kunne oppfylle vilkår for en bindende avtale etter avtaleloven.¹⁰ En nærmere sammenligning kan kanskje være avgivelsen av et tilbud, men heller ikke dette vil være nært nok til at en erklæring i seg selv faller innunder rettsområdet.

Som metode vil kontraktsretten likevel kunne gi noen rettslige utgangspunkter som kan være givende ved tolkningen av en slik tekst, og jeg vil derfor trekke veksler herfra når jeg tolker innholdet i personvernerklæringene. Det generelle utgangspunktet ved kontraktstolkning vil være hvordan teksten fremstår for en alminnelig person. Jeg vil i analysen ta utgangspunkt i ordlyden og den alminnelige språklige forståelsen erklæringene gir uttrykk for, slik kontraktsrettslig metode foreskriver. Da erklæringene er skrevet med utgangspunkt i personopplysningsloven vil det videre være nærliggende å forstå teksten i lys av lovens bestemmelser.

Jeg vil i oppgavens siste del, kapittel 5, stille spørsmålet om erklæringer kan gi hensiktsmessig og tilstrekkelig informasjon. Jeg vil her drøfte erklæringene i utvalget mer kritisk opp mot om brukerne faktisk får den informasjonen de behøver for å verne egne personopplysninger, gjennom å knytte sammen de rettskilder som både kan begrunne bruken og innholdet med informasjonen som er gitt. Jeg vil til slutt komme med noen generelle betraktninger, og nevne enkelte utfordringer som oppstår ved bruken av personvernerklæringer.

¹⁰ Se noe mer om denne diskusjonen i kap. 4.6.1.

2.3 Rettskilder og juridisk metode

2.3.1 Lovgivning og EU-direktiv

Det vil være naturlig å ta utgangspunkt i personvernlovgivningen i sin helhet, med personopplysningsloven (pol.) med forskrifter som utgangspunkt for en analyse av personvernerklæringer. Innen rettsområdet personvern er rettskildebildet noe spesielt. Rettsområdet påvirkes både av internasjonale rettskilder, og av nasjonal administrativ praksis. Personopplysningsloven er en implementering av EUs personverndirektiv¹¹ i norsk rett. Personverndirektivet er innlemmet i EØS-avtalen, og Norges utøvelse av personvernlovgivningen må utøves i samsvar med dette, jfr. EØS-loven,¹² slik forarbeidene også forutsetter.¹³ Der jeg møter tolkningsutfordringer i personopplysningsloven vil jeg derfor berøre de enkelte artikler og direktivets fortale. Oppgaven avgrenses likevel til norsk rett, da utvalget består av erklæringer rettet mot norske brukere. Jeg vil ikke bruke noe tid på dommer fra EU-domstolen, selv om disse klart kan være relevante.

Forsikringsvirksomhet spesielt reguleres på grunnlag av forsikringsvirksomhetsloven(forsvl.),¹⁴ og avtalen mellom forsikringsselskapet og kunden er regulert av forsikringsavtaleloven(fal.).¹⁵ Disse særlovene har ingen spesialregler for behandling av personopplysninger, til sammenligning med for eksempel finansvirksomhet hvor spesialregler forekommer. Personopplysningsloven gjelder derfor fullt ut for forsikringsvirksomhet. Forsikringsvirksomhet er konsesjonsbelagt, jfr. personopplysningsforskriften¹⁶ (pof.)§ 7-2, og både If og Storebrand er underlagt konsesjon for sin behandling av personopplysninger. Særskilte krav følger av konsesjonen.

¹¹ Direktiv 95/46/EF

¹² Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde av 27.november 1992 nr.109

¹³ Ot. prp. nr.92 (1998-1999) s.14-15.

¹⁴ Lov om forsikringsselskaper, pensjonsforetak og deres virksomhet mv. av 10. juni 2005 nr.44

¹⁵ Lov om forsikringsavtaler av 16.juni 1989 nr.69

¹⁶ Forskrift om behandling av personopplysninger av 15. desember 2000 nr.1265

If og Storebrand utøver virksomhet både i Norge og i andre land, og det vil være nødvendig å klarlegge at den norske personopplysningsloven kommer til anvendelse. Personopplysningsloven gjelder behandlingsansvarlige som er etablert i Norge, jfr. pol.§ 4. Behandlingsansvarlig er den parten som bestemmer formålet med innsamlingen, jfr. pol.§ 2 nr.4, og herunder har det overordnede ansvar for etterlevelse av lovgivningen.¹⁷ Dette kan være en juridisk person,¹⁸ for eksempel et AS, og i praktisk forstand knyttes det som regel til organisasjonsnummer. I et konsern vil det dermed være minst én behandlingsansvarlig per datterselskap. For å være etablert i Norge kreves at det utøves en viss aktivitet i Norge, gjennom en fast organisatorisk infrastruktur, og for et ubestemt tidsrom.¹⁹

En analyse av If utgjør en utfordring da selskapet er registrert som et NUF, jfr. forsvl.§ 14-1, og er en del av et svensk/finsk konsern.²⁰ Pol.§ 4 forstås som at personopplysningsloven ikke gjelder for behandlingsansvarlige som er etablert i andre EØS-land, selv om virksomheten og behandlingen er rettet mot norske brukere.²¹ I forarbeidene uttales det at:

"Strukturens rettslige status – f.eks. hvilken sammenslutningsform som er nyttet – er ikke avgjørende. Avgjørende er om den behandlingsansvarlige har tilstrekkelig tilknytning til Norge til å være etablert slik uttrykket forstås ut fra en alminnelig språklig forståelse. Dersom et utenlandsk selskap har et datterselskap som driver virksomhet i Norge, er tilknytningskravet åpenbart oppfylt slik at datterselskapet er etablert her. Det samme gjelder utenlandske selskapers filialer i Norge".²²

¹⁷ Schartum(2012) note 10.

¹⁸ Schartum(2011) side 149-150.

¹⁹ Schartum(2012) note 29.

²⁰ If(2013 c)

²¹ Schartum(2012) note 29.

²² Ot.prp.nr.92 (1998-1999) s.105

Her får en inntrykk av at et NUF, som en filial av et utenlandsk selskap, vil være underlagt personopplysningsloven. Imidlertid kan en finne en viss motstrid mellom norsk rett og EU-rett omkring dette spørsmålet. Selskapsformen NUF er etablert som følge av prinsippet om fri etableringsrett innen EU, og for en norskregistrert utenlandsk filial, NUF, vil det i utgangspunktet være det utenlandske selskapet som i prosessuell forstand er rettssubjektet.²³ Det er likevel et mulig unntak nettopp for norske filialer av utenlandske forsikringsselskaper, jfr. Rt-2005-451 og forsvl.§ 14-2, hvor førstvoterende ga den norske filialen av et forsikringsselskap partsevne.²⁴ Hvorvidt dette står seg mot EU-retten er usikkert.

I EUs personverndirektiv²⁵ (heretter: personverndirektivet) art.4 nr.1 er regelen at:

"Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State;"

Nasjonal lovgivning skal anvendes. Likevel står det videre i samme artikkel at:

"when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable".

Sammenholdt med pol.§ 4 vil en kunne stille spørsmål om et europeisk selskap som står bak et NUF vil være underlagt norsk rett, eller om de kun behøver å forholde seg til sitt lands gjennomføring av personverndirektivet. I personverndirektivets art.28 nr.6, jfr.nr.3, oppstilles regelen om at de nasjonale myndigheter kan anvende andre lands personvernlov-

²³ Reiersen(2010)

²⁴ Reiersen(2010)

²⁵ Direktiv 95/46/EF

giving på sitt territorium. Jamført med denne regelen kan tilstanden tyde på at et NUF er underlagt opprinnelseslandets lovgiving innen EØS, på tross av avgjørelsen i Rt-2005-451 og forarbeidene til § 4.

I sak PVN-2011-06 ConocoPhillips, hvor det er et amerikansk NUF som er part, legger Personvernnemnda til grunn at:

"det amerikanske selskapet og NUF'et er samme juridiske enhet. En norsk avdeling av et utenlandsk selskap er et utenlandsk foretak, jf foretaksregisterloven § 1-2, men det er registreringspliktig i Norge når det driver næringsvirksomhet her, jf foretaksregisterloven § 2-1, annet ledd."

En må likevel skille mellom land innenfor eller utenfor EØS, jfr. pol.§ 4 (2), og ConocoPhillips-saken vil derfor ikke være avgjørende i dette tilfellet.

Forhold som taler for at en likevel vil kunne legge til grunn norsk rett foreligger. If har hatt en sak oppe for Personvernnemnda, uten at spørsmålet om selskapets stauts kom opp.²⁶ Datatilsynet har heller ikke selv problematisert forholdet mellom forsvl.§ 14-1 og § 14-2, og pol.§ 4, da konsesjon ble tildelt If for forsikringsvirksomhet, og If selv henviser til norsk lovgiving på sine nettsider. Rettstilstanden fremstår som uklar. Uten at jeg tar endelig stilling til hvorvidt If er underlagt norsk lovgiving vil jeg i det følgende støtte meg på forarbeidenes uttalelse om at struktur ikke er avgjørende, det faktum at If selv henviser også til norsk lovgiving i sin erklæring, og at informasjonen i erklæringen utelukkende er rettet mot det norske markedet.

Storebrand er på sin side et allmennaksjeselskap, og behandlingsansvarlig for forsikringsvirksomheten er det norskregistrerte datterselskapet Storebrand Forsikring AS.²⁷ Store-

²⁶ PVN-2010-06

²⁷ Storebrand(2013 b)

brand sin virksomhet må sies å klart falle innenfor det stedlige virkeområdet for personopplysningsloven.

All behandling av personopplysninger som skjer ved bruk av elektroniske hjelpemidler vil være regulert av personopplysningsloven, jfr. lovens § 3 (1) bokstav a. "*Behandling*" er definert i loven som "*enhver bruk av personopplysninger*", jfr. § 2 nr.2, slik at virksomheter som på et eller annet vis benytter seg av opplysninger om brukerne sine vil være underlagt personopplysningsloven.

Både If og Storebrand vil således være underlagt norsk rett, og erklæringene vil i det følgende drøftes i lys av norsk lovgivning.

2.3.2 Praksis

Norsk rettspraksis vil være naturlig å se hen til ved tolkningsutfordringer i loven, men det er sparsomt med avgjørelser av Høyesterett i prinsipielle personvernsspørsmål. Høyesterett har heller ingen direkte avgjørelser som kan kaste lys over de aktuelle bestemmelser i videre grad enn det andre rettskilder kan.

Av praksis vil jeg først og fremst ta for meg avgjørelser fra Personvernemnda. Personvernemnda er et uavhengig forvaltningsorgan som avgjør klager over Datatilsynets avgjørelser, med hjemmel i pol. § 43. Det er presisert i forarbeidene at det skal legges vekt på administrativ praksis ved tolkning av loven.²⁸

Datatilsynet er på sin side et uavhengig forvaltningsorgan, som i tillegg til å være et tilsyns- og kontrollorgan gir rådgivende uttalelser om personvern, jfr. pol. § 42. Datatilsynets uttalelser vil dermed være en relevant kilde til informasjon om tolkningsspørsmål. Der Personvernemnda har avgjort spørsmål vil imidlertid deres tolkning vektas over Datatilsynet, da

²⁸ Ot.prp. nr.92 (1998-1999) s.101

de er klageorgan for Datatilsynets avgjørelser. Videre vil vilkår gitt i konsesjon av Datatilsynet trekke opp rammer for behandlingsgrunnlaget for personopplysninger, og således være et relevant rettskildemateriale for å forstå innholdet i erklæringene. Slik konsesjon er gitt i vårt tilfelle, og både standardkonsesjonen etter personopplysningsloven for forsikringsvirksomhet og for finansvirksomhet vil bli referert til.²⁹

2.3.3 Internasjonale rettskilder

Enkelte internasjonale rettskilder vil på grunn av personverndirektivets implementering i personopplysningsloven ha relevans i tillegg til personverndirektivet i seg selv. En slik særskilt kilde er Artikkel 29-gruppen, et uavhengig EU-organ med medlemmer fra blant annet EU-landenes tilsynsmyndigheter, hjemlet i personverndirektivet artikkel 29. Gruppen fremstår som en kombinasjon av å være en representant for de enkelte EU-lands personverntilsyn, og å være et selvstendig rådgivningsorgan for praktiseringen av personverndirektivet. Gruppen har en rekke uttalelser, som i praksis tillegges stor vekt.³⁰ Artikkel 29-gruppen er en viktig part i samkjøringen av lovverket for de land som har implementert personverndirektivet. Norge er ikke medlem av gruppen, men har observatørstatus.³¹ Datatilsynet forholder seg med det til de uttalelser og råd som gruppen kommer med, jfr. gruppens hjemmel i personverndirektivets artikkel 29, som en kilde for avklaring og rådgivning av personvernspørsmål. For utøvelse og forståelse av direktivet, herunder også av den norske personopplysningsloven, vil uttalelser fra Artikkel 29-gruppen kunne ha stor vekt, og vil henvises til i den følgende drøftelsen.

Et annet internasjonalt organ er International Conference of Data Protection and Privacy Commissioners. Konferansen er et årlig forum for diskusjon av personvern, og samler stater og internasjonale organisasjoner fra hele verden. Forumet vil ikke ha samme status eller

²⁹ Datatilsynet(2011 b), Datatilsynet \ (2005)

³⁰ Schartum(2012) note 1.

³¹ Jfr. Meld. St.11 (2012–2013) side 22.

rettskildemessig relevans som Artikkel 29-gruppen, og vil vektes deretter, men resolusjoner avgitt av forumet anerkjennes av EU som en kilde for rådgivning innen personvern.³²

2.3.4 Særskilt juridisk litteratur, bransjeorganer og rådgivning

Som et siste rettskildemessig punkt vil jeg nevne særskilte veiledningstekster som er laget av enkelte rådgivende organer konkret om personvernerklæringer. Det er typisk bransjeorganer, slik som Electronic Frontier Foundation,³³ som kommer med slike, eller det kan være internasjonale samarbeidsorganer innen personvern som utformer dem, slik som Artikkel 29-gruppen. Jeg vil komme tilbake til slike i kapittel 3.3.

Når bransjeorganer kommer med rettslige veiledere kan nok ikke dette sies å være omfattet av det som regnes som tradisjonell juridisk litteratur. Det er derfor begrenset hvilken rettskildemessig vekt de vil ha, det avgjørende kan sies å være hvilket organ som står bak. Noe relevans vil de likevel ha. Det er ofte generelle anbefalinger, i stor grad basert på de samme personvernprinsipper som vi har i Norge, og de kan bidra til å identifisere aktuelle reelle hensyn. Slike veiledere blir også henvist til i offentlige lovutredninger,³⁴ noe som kan begrunne relevansen. Jeg vil referere til slike veiledere der de etter min vurdering har relevante bidrag til analysen.

³² Se forslag til ny personvernforordning, Forordning 2012/0011 (KOM) art.11

³³ Electronic Frontier Foundation(2008)

³⁴ NOU 2009:1 kapittel 13.5.4.1.

3 Den rettslige begrunnelsen for bruken av personvernerklæringer

3.1 Hva er en personvernerklæring?

Personvernerklæringer er et generelt tekstdokument på en nettside³⁵ som fremstår for en alminnelig leser som informasjon om hvordan virksomheten bak den konkrete nettsiden forholder seg til personvern, og kanskje som et løfte om at loven følges. Et par fellestrekk for slike tekster kan trekkes frem. Det som gjentar seg er at det er tekst publisert på en nettside, under overskrifter som "*personvernpolicy*", "*informasjon om behandlingen av personopplysninger*", "*slik behandler vi dine personopplysninger*", og lignende. Teksten tar for seg en virksomhets behandling av personopplysninger; noen ganger svært kort, andre ganger over flere avsnitt og sider. Typisk gis informasjon om selve behandlingen i virksomheten, rettigheter for brukeren, og kommunikasjonsmåter med virksomhetene. Teksten kan også være spredt ut over nettsiden, slik at brukeren av nettsiden må lese på flere steder.³⁶

37



³⁵ Se vedlegg for eksempler.

³⁶ Datatilsynet(2011 a)

³⁷ Skjermdump av erklæringen til If, If(2013 a)

Innholdet i en erklæring vil kunne variere avhengig av hva slags behandling som forekommer i virksomheten. Opplysninger som innhentes av en virksomhet, eller gjennom en nettside, kan være et mangfold av opplysninger, og kan innhentes og behandles på ulike måter. Begrepet "*behandling*" benyttes om både innsamling, lagring, og all annen bruk av personopplysninger, jfr. pol.§ 2 nr.2.

For at det skal skje innsamling må det være en viss aktivitet fra den behandlingsansvarliges side.³⁸ Det er likevel ikke slik at bevegelse på et nettsted ikke medfører innsamling av personopplysninger. Dersom nettstedet er lagt opp slik at en kan gi fra seg opplysninger må aktivitetskravet fra den behandlingsansvarlige sies å være oppfylt. Det avgjørende i følge forarbeidene for om innsamling har skjedd i en slik sammenheng, vil være hvorvidt det "*reelt sett er [oppstått] et personvernbehov for varsling*".³⁹ Både If og Storebrand har slike systemer for innhenting av informasjon gjennom sine nettsider, se kapittel 4.3

En personopplysning er på sin side "*opplysninger og vurderinger som kan knyttes til en enkeltperson*", jfr. pol.§ 2 nr.1. Eksempler er elektroniske spor gjennom informasjonstjenester på en nettside, innsending av opplysninger gjennom nettskjema eller gjennom betalingssystemer. Mer alminnelig er kanskje gjennom post eller telefonsamtaler. Et skille går mellom de virksomheter som kun har brukeraktivitet gjennom en nettside, og som ikke egentlig benytter personopplysninger som en del av virksomheten, og de som aktivt benytter personopplysninger. Derfor vil informasjonen som gis i en erklæring kunne avhenge av hva slags virksomhet som utøves, og hvordan personopplysninger behandles. Se mer om dette i kapittel 5.2.3.

En virksomhet vil også behandle opplysninger om egne ansatte, men formen tilsier at erklæringer som regel ikke har denne gruppen som målgruppe. For de utvalgte virksomhetene i denne analysen er mottakeren ofte kunder, og virksomhetene sitter da med personopp-

³⁸ Blixrud(2010) side 106.

³⁹ Jfr. Ot.prp. nr.92 (1998-1999) side 120.

lysninger om vedkommende. Den som en personopplysning kan knyttes til, kalles i pol. for "*registrert*", jfr. pol.§ 2 nr. 6. En kunde vil derfor tilsvare den som etter personopplysningsloven forstås som "*registrert*". I og med at det kan forekomme innsamling også fra brukere som ikke er kunde av virksomheten, vil nettopp skillet mellom en registrert, en bruker av en nettside, og en kunde, i enkelte tilfeller være viktig å presisere. Begrepene kunde, bruker og registrert vil også kunne benyttes om samme person.

I det videre vil *personvernerklæringer* refereres til som et publisert nettdokument, som samlet tar for seg behandlingen av personopplysninger i en virksomhet, og hvor mottakeren for teksten er virksomhetens egne kunder og/eller brukere av nettsiden.

3.2 Forholdet til aktuell lovgivning

Lovgivningen er taus når det kommer til personvernerklæringer, det foreligger ingen materiell lovhjemmel som sier at en virksomhet må ha en slik erklæring på sin hjemmeside. En må derfor lete litt i rettskildene for å finne et mulig grunnlag for bruken av personvernerklæringer. Under drøftelsen av innholdet i personvernerklæringer vil vi se at selve innholdet i disse har sitt fundament i krav som stilles i personvernlovgivningen. Personopplysningsloven kan derfor legge et grunnlag for forståelse også for bruken av en erklæring, sammen med annen bakgrunnsrett.

Personopplysningslovens hovedformål er nedfelt i § 1 (1): Å "*beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger*". Vern mot krenkelse av individet må derfor sees på som hovedhensikten med loven. Bestemmelsen er først og fremst en tolkningsbestemmelse uten noe egentlig materielt innhold.⁴⁰ I andre ledd understrekes det at behandling av personopplysninger skal skje "*i samsvar med grunnleggende personvern hensyn*". Pol.§ 1 gir liten videre veiledning i hva som er slike grunnleggende personvern hensyn annet enn privatlivets fred, integritet og tilstrekkelig kvalitet på person-

⁴⁰ Johansen(2001) side 66.

opplysninger. Lovens andre bestemmelser gir noe videre veiledning gjennom de ulike hensyn bak reglene. For eksempel må det som hovedregel samtykkes til behandling for at behandlingsgrunnlag skal foreligge, jfr. pol.§ 8 (1), frivillighet er derfor et sentralt hensyn.

Akkurat hvilke prinsipper og hensyn som begrunner personvernet er i liten grad behandlet i personopplysningslovens forarbeider. I NOU 1997: 19 uttales at "*Personvern er primært en beskyttelse av et samtykke til en kanal*", og at privatlivets fred primært er en beskyttelse av "*muligheten til å samtykke*".⁴¹ Noen av de bakenforliggende hensyn er videre omtalt i personverndirektivet, og i juridisk teori.

I personverndirektivets fortale presiseres at retten til privatlivets fred skal vernes gjennom nasjonal lovgivning om behandling av personopplysninger.⁴² Det presiseres at opplysninger som er av en slik art at de kan krenke grunnleggende friheter eller privatlivets fred, med få unntak ikke bør behandles uten uttrykkelig samtykke fra den berørte.⁴³

I juridisk teori er interesseteorien viktig; en modell som tar sikte på å beskrive hvilke interesser personvernet er grunnlagt på. For så vidt gjelder personvernerklæringer, kan de såkalte "*individuelle interesser*" være særlig interessant å trekke frem. Utgangpunktet for den individuelle tilnærmingen er det normative spørsmålet om hvordan et individ vil vektlegge personvern hensyn opp mot andre hensyn.⁴⁴ Gjennom dette perspektivet fremstår hensynet til selvbestemmelse og autonomi som viktig. Samtykke og frivillighet vil dermed være grunnleggende for individets vern.⁴⁵ For å sikre frivillighet og selvbestemmelse, kan det stilles et krav om et tillitsforhold mellom den som behandler opplysninger og en som har

⁴¹ NOU 1997:19 side 224, vedlegg 6.

⁴² Fortalen punkt 10.

⁴³ Fortalen punkt 33.

⁴⁴ Schartum(2011) side 42-43.

⁴⁵ Schartum(2011) side 161.

gitt fra seg personopplysninger.⁴⁶ I denne sammenheng vil innsyn i behandlingen være et viktig middel, og innsyn er derfor et viktig prinsipp innen personvern.⁴⁷ Behovet for innsyn kan begrunnes på flere måter. Innsyn medfører åpenhet om hvordan en virksomhet driver, men gir også grunnlag for å vurdere om en vil gi fra seg personopplysninger. På et mer overordnet plan synes retten til innsyn dermed å forene elementene samtykke, tillitt og åpenhet om behandlingen.

Vi ser at samtykke er et gjennomgående tema i de ulike rettskilder, og det kan betraktes som et gjennomgående prinsipp i personvernlovgivningen at behandling av personopplysninger skal basere seg på samtykke og frivillighet, selv om unntak forekommer.⁴⁸ Et samtykke må være *"frivillig, uttrykkelig og informert"*, jfr. pol.§ 2 nr. 7. Den registrerte må være informert om behandlingen, og *"den registrerte må gis tilstrekkelig informasjon slik at vedkommende vet hva det samtykkes i"*.⁴⁹ Det er altså et informasjonsbehov ved behandling av personopplysninger.

Personopplysningsloven hjemler da også i § 19 og § 20 nettopp en informasjonsplikt før innsamling tar til, og av *"eget tiltak"* fra den behandlingsansvarlige, jfr.§ 19(1). Informasjonsplikten omfatter både informasjon om at det faktisk samles inn og behandles personopplysninger i den aktuelle virksomhet, og konkrete forhold som aktivt må opplyses om *"før"* behandling, jfr. pol.§ 19(1) bokstav a-e. Dette inkluderer hvem som er behandlingsansvarlig, formålet, om opplysningene vil bli utlevert og til hvem, om det er frivillig å gi fra seg opplysningene, og annet som gjør den registrerte i stand til å *"bruke sine rettigheter"* etter personopplysningsloven.

⁴⁶ Schartum(2011) side 50.

⁴⁷ Jfr. Ot.prp. nr.92 (1998-1999) s. 20.

⁴⁸ Jfr. blant annet pol.§ 8 1.setning, 2.alternativ.

⁴⁹ Jfr. Ot.prp. nr.92 (1998-1999) s.104.

Rett til innsyn utover denne informasjonen er hjemlet i pol.§ 18. Innsynsregelen gir i bestemmelsens første ledd innsynsrett for allmennheten, og i andre ledd en rett for den enkelte registrerte. Slik informasjon må det kreves innsyn i, og virksomheten kan kreve at det fremsettes skriftlig skrav, jfr. pol.§ 24. I motsetning til informasjonsplikten som foreligger etter § 19 og § 20 behøver virksomheten således ikke å gi innsyn av eget tiltak. Allmennhetens innsynsrett er i noen grad sammenfallende med informasjonsplikten, jfr.§ 19(1), og omfatter formålsangivelse, behandlingsansvarlig og utlevering. Men også en beskrivelse av hvilke typer personopplysninger som behandles og hvor de hentes fra kan det kreves innsyn i, jfr.§ 18(1) bokstav a-f. For en registrert utvides retten til å gjelde hvilke opplysninger som behandles, og informasjon om sikkerhetstiltak ved behandlingen, i tillegg til en utdyping av de forhold som gis innsyn i etter første ledd, jfr.2. og 3.ledd.

I pol.§ 24 fastslås det at den informasjonen en virksomhet er pålagt å gi, kan kreves skriftlig hos den behandlingsansvarlige, eventuelt dennes databehandler. Altså foreligger det ikke et krav om at informasjon som er pålagt å gi, i utgangspunktet skal gis skriftlig. Likevel vil en virksomhet komme et slikt krav fra enten en registrert eller fra allmennheten i forkant, ved å gi informasjon i en erklæring. Selv om bestemmelsen tar for seg hvordan denne informasjonen skal gis, sier den ikke annet om dette enn at informasjonen kan kreves skriftlig. Det foreligger derfor ikke noen generell hovedregel om formkrav for informasjon til de registrerte, men vi ser at informasjon må gis på en eller annen måte.

Datatilsynet uttaler i sin rapport om personvernerklæringer om informasjonsplikten i § 19 at en *"viktig kanal for denne typen informasjon er virksomhetens nettsider"*.⁵⁰ Informasjonsplikten i pol.§ 19 kan likevel ikke gi en tilstrekkelig begrunnelse verken for innhold eller bruken av personvernerklæringer. Bestemmelsen vil i utgangspunktet oppstille et informasjonskrav for hver behandling som foretas, mens en erklæring gis én gang og er noe en bruker selv må oppsøke. Likevel er det særlig denne bestemmelsen som trekkes frem av

⁵⁰ Datatilsynet(2011 a)

Datatilsynet i forbindelse med personvernerklæringer, ikke innsynsregelen i § 18, på tross av at det er denne som omhandler allmennheten.

Det kan tenkes at informasjonsplikten, jfr. § 19, i noen spesielle tilfeller kan oppfylles gjennom en personvernerklæring. Dersom innsamling skjer over tid antas det å være tilstrekkelig at den registrerte informeres ved første gangs innsamling, forutsatt at det informeres om at det også senere vil samles inn personopplysninger.⁵¹ Ved innsamling av personopplysninger utelukkende gjennom internettaktivitet vil det ikke være noen forutgående direkte kontakt mellom brukeren av nettstedet og den aktuelle virksomheten, samtidig som informasjon må gis på en eller annen måte. For slike situasjoner uttales det i forarbeidene at varsling kan gjennomføres ved at det opplyses om behandlingen av opplysningene gjennom *"lett tilgjengelig elektronisk informasjon før kontakten med nettstedet opprettes"*.⁵²

For forsikringsvirksomhet er det i konsesjonen et tilleggsvilkår til § 19 om hvordan informasjon skal gis, og når:

*"Den registrerte må få skriftlig informasjon om alle sider av behandlingen før den iverksettes, jf. personopplysningsloven § 19. For muntlig inngåtte forsikringsavtaler, gis skriftlig informasjon senest ved oversendelse av skriftlig avtalebekräftelse."*⁵³

Det foreligger altså et skriftlighetskrav for informasjonsplikten gitt av forsikringsselskaper, og utvalget i oppgaven vil ikke være i en slik posisjon hvor informasjonsplikten kan oppfylles utelukkende gjennom en personvernerklæring. Bruken av personvernerklæring kan derfor heller ikke for If og Storebrand begrunnes utelukkende gjennom personopplysningsloven. Personvernerklæringer fremstår likevel som et av flere redskap i oppfyllelsen av

⁵¹ Johansen(2001) side 161.

⁵² Ot.prp.nr.92 (1998-1999) side 119.

⁵³ Datatilsynet(2005)

blant annet informasjonsplikten i personopplysningsloven, se kapittel 5.1 for videre drøftelse.

3.3 Den videre rettstilstanden

Selv om bestemmelsene som hittil er gjennomgått til en viss grad kan begrunne et behov for personvernerklæringer, finner vi ikke hele forklaringen i personopplysningsloven. Det kan være oppklarende å se hen til blant annet Artikkel 29-gruppens uttalelser om erklæringer, og andre rettskilder.

Artikkel 29-gruppen har flere uttalelser om hvordan en behandlingsansvarlig bør gi brukere og registrerte informasjon om behandlingen av personopplysninger. I Recommendation 2/2001 anbefales det å informere om behandling av personopplysninger "*directly on the screen*", og at informasjonen er "*directly accessible on the home page of the site and anywhere where personal data are collected on-line*".⁵⁴ Rådet er altså at virksomheter informerer om behandlingen på sin hjemmeside, typisk gjennom en personvernerklæring tilgjengelig fra forsiden. Uttalelsen knytter seg til artiklene 6, 7, 10 og 11 i personverndirektivet, artikler som tar for seg når, hvordan og hva slags informasjon som en bruker har krav på. Innholdet i disse artiklene er i stor grad implementert i pol.§ 8, § 19 og § 20, så en ser her at informasjonsplikten i § 19 gjentas som en begrunnelse for personvernerklæringer også av Artikkel 29-gruppen.

I Opinion 10/2004⁵⁵ følges 2001-uttalelsen opp, og gruppen gjennomgår her hvordan og hva slags informasjon som skal gis i situasjoner hvor virksomhet utøves over internett. Uttalelsen knyttes også her opp til de samme artikler i personverndirektivet som ved forrige uttalelse. Om behovet om en enhetlig praksis for å gi informasjon, og bruk av personvernerklæringer, uttaler Artikkel 29-gruppen at virksomheter har utfordringer ved oppfyllelsen

⁵⁴ WP 43

⁵⁵ WP 100

av reglene om informasjonsplikten, og at det er et behov for å øke borgeres kunnskap om personvern generelt. Informasjonen bør presenteres med et meningsfullt innhold og på en hensiktsmessig måte, og utformingen av innholdet må tilpasses leserne. På denne bakgrunn foreslås det at informasjon skal gis som tekst med et enkelt språk, i en layout som er lett tilgjengelig og tilpasset de ulike brukerne av nettsiden.⁵⁶ Her finner vi igjen skillet mellom en bruker av en nettside og en som også er kunde, og uttalelsen presiserer at ulike brukere har behov for ulik informasjon. Imidlertid finner en ikke igjen noen henvisning til en innsynsrett for allmennheten, slik at innsynsregelen i pol.§ 18 heller ikke her fremheves i denne sammenheng.

Også andre organer kommer med uttalelser om personvern. I november 2009, ble det i Madrid vedtatt en resolusjon om internasjonale standarder for beskyttelse av personvernet av International Conference of Data Protection and Privacy Commissioners. Ett av de nedfelte prinsipper i resolusjonen av 2009, punkt 10 nr. 6, er prinsippet om åpenhet, hvor det foreslås at der personopplysninger samles inn over internett kan informasjonsplikten og åpenhet overfor de registrerte oppfylles gjennom en personvernerklæring.⁵⁷ Prinsippet om åpenhet som anerkjennes her kan forstås som en side til prinsippene om innsyn, samtykke og tillitt, og en ser her hvordan slike prinsipper bygger rammer både for personvernlovgivningen og anbefalt praksis.

Ved siden av de mer offisielle rådgivende organ, lager også enkelte andre organisasjoner veiledere om personvernerklæringer, først og fremst i form av maler og tips til virksomheter om utformingen. Norske myndigheter har selv vist til slike i utarbeidelsen av lovforslag. I NOU 2009:1 vises det til en veileder Electronic Frontier Foundation (heretter:EFF) har laget, som heter "Best Practices for Online Service Providers".⁵⁸ I utredningen ble det lagt

⁵⁶ WP 100

⁵⁷ International Conference of Data Protection and Privacy Commissioners(2009)

⁵⁸ Electronic Frontier Foundation(2008)

frem et utkast til en plakat om regler for god nettskikk. En ser her at prinsippet om åpenhet gjentas, gjennom ett av de konkrete forslagene:

"Ethvert medium som samler inn og/eller behandler personopplysninger om sine brukere skal ha en publisert personvernerklæring som sikrer transparens når det gjelder behandling av personopplysninger".⁵⁹

Det uttales av EFF at en erklæring skal inneholde "*what purposes they will use it for, how long they will keep it, whom (if anyone) they will share it with, and under what terms*".⁶⁰ Dette tilsvarer hva vi ser anbefalt ellers.

Datatilsynet skal bistå i utarbeidelsen av bransjevise atferdsnormer, jfr. pol.§ 42 (3) nr.6. På bakgrunn av de rådgivende uttalelser fra blant annet Artikkel 29-gruppen anbefaler Datatilsynet både offentlige og private virksomheter å ha en personvernerklæring tilgjengelig.⁶¹ Personvernerklæringer nevnes også som en del av normen om innebygget personvern. Et innebygget personvern vil tilsi at en virksomhet søker å ivareta hensynet til personvern i alle faser av et system eller løsning. Et av de stegene som må være på plass i et slikt system er åpenhet utad, og en informativ personvernerklæring er et godt bidrag til dette.⁶²

Da Datatilsynet foretok en undersøkelse av antallet virksomheter som benyttet seg av en personvernerklæring, hadde alle de private virksomhetene i utvalget dette, mens de offentlige virksomhetenes nettsider ble lite brukt til formidling av personopplysningsbehandling.⁶³

⁵⁹ NOU 2009:1 side 124.

⁶⁰ Electronic Frontier Foundation(2008)

⁶¹ Datatilsynet(2011 a)

⁶² Datatilsynet(2013 d)

⁶³ Datatilsynet(2011 a)

I samme rapport uttales det at personvernerklæringer er en god måte å informere brukerne på, gjennom å være nyttig informasjon for brukerne, samtidig som det er lite byrdefullt for virksomhetene. Videre trekker de frem som en fordel ved bruken av slike det at informasjon gis samlet. Brukerne får bedre oversikt, og har tilgang på informasjonen. Dersom det ikke er en lenke til informasjon om personvern på forsiden, og brukerne vil måtte søke etter informasjon i nettsidens søkefelt, vil mye informasjon kunne forsvinne eller være utilgjengelig.⁶⁴ Virksomhetene vil heller ikke ha mulighet til å "gjemme bort" informasjon fra brukerne i like stor grad dersom forventningen er at all relevant informasjon om personvern står i dette dokumentet som på nettsiden heter personvernerklæring.

I Meld. St.11 (2012-2013) kapittel 7.4 gjennomgås plikten til å informere om behandling av personopplysninger, og det anføres et behov for å styrke denne.⁶⁵ Det samme gjøres i EUs nye forordningsforslag om personvern, her ved at informasjon skal være lettere tilgjengelig, og forståelig, for brukerne.⁶⁶ I ny artikkel 11 foreslås inntatt:

"[T]he obligation on controllers to provide transparent and easily accessible and understandable information, inspired in particular by the Madrid Resolution on international standards on the protection of personal data and privacy".⁶⁷

Altså følges Madrid-resolusjonens uttalelser opp om at informasjonsplikten og åpenhet overfor de registrerte kan oppfylles gjennom en personvernerklæring, jfr. resolusjonens punkt 10 nr. 6.⁶⁸ Det gjentas således på flere politiske plan et ønske om en styrking av informasjonen brukere får når de deler personopplysninger med virksomheter.

⁶⁴ Datatilsynet(2011 a)

⁶⁵ Meld. St.11 (2012-2013) side 62.

⁶⁶ Forordning 2012/0011 (KOM) og Meld. St.11 (2012-2013) side 65, 1.spalte

⁶⁷ Forordning 2012/0011 (KOM) art.11

⁶⁸ International Conference of Data Protection and Privacy Commissioners(2009)

Artikkel 29-gruppen kom også nylig med en uttalelse om informasjon for applikasjoner til mobil, hvor det uttales at:

"At the very least, every app should have a readable, understandable and easily accessible privacy policy, where all the above mentioned information is included".⁶⁹

Personvernerklæringer er dermed på vei inn for de fleste plattformer for internettbruk, og prinsippene om at forståelig og lett tilgjengelig informasjon skal gis opprettholdes og se-menteres.

Det kan bemerkes at så lenge det ikke foreligger klare materielle hjemler, og ingen klart utviklet norm for verken oppsett eller innhold, vil det ikke foreligge noen mulighet for på-legg eller sanksjon for virksomheter som mangler en slik. Åpen kritikk fra Datatilsynet kan nok i seg selv også ha en viss sanksjonerende virkning gjennom potensielt negativ PR, og medføre at brukerne både blir bevisste og skeptiske til nettsteder uten personvernerklæ-ringer. Se kapittel 5.2.5 for videre diskusjon.

De rettskilder, anbefalinger og utgangspunkter som er redegjort for ovenfor vil antas å angi en begrunnelse for selve bruken av personvernerklæringer, og kan også trekkes inn i drøf-telsen av selve innholdet. Det er likevel ikke slik at det foreligger et entydig, klart grunnlag for bruken av erklæringer. Derfor vil jeg ikke utelukke at virksomheter benytter slike på bakgrunn av en respekt for tillitsforholdet mellom en registrert og en virksomhet som skal behandle personopplysninger.

⁶⁹ WP 202

4 En empirisk undersøkelse av innholdet i personvernerklæringene til If og Storebrand

4.1 Innledning, tilgjengeligheten til erklæringene

I det foregående er en begrunnelse for selve bruken av erklæringer redegjort for. I det følgende vil det være innholdet i erklæringene som er i fokus. At personvernerklæringer ikke har en materiell hjemmel gjør det utfordrende å drøfte innholdet. Det rammeverket som ble redegjort for i kapittel 3, er det samme erklæringenes innhold kan tolkes ut fra. Likevel vil det være viktig å huske på at personvernerklæringer informerer generelt, det er ikke en presis angivelse av hver enkelt behandling som forekommer i virksomheten.⁷⁰

Aller først kan det være interessant å undersøke tilgjengeligheten av de aktuelle erklæringene. Uten tilgang på erklæringene vil innholdet være irrelevant. Brukerne av henholdsvis www.if.no og www.storebrand.no må selv trykke på en lenke som heter henholdsvis "*Behandling av personopplysninger*"⁷¹ og "*Informasjon om behandling av personopplysninger*"⁷² på forsiden av nettstedene, for å få tilgang på erklæringene. If har i tillegg en tekst publisert med lenketittel "*Cookies*",⁷³ hvor de har informasjon rettet spesifikt mot brukerne av nettsiden.

Det uttales av Artikkel 29-gruppen i Recommendation 2/2001,⁷⁴ hvor personvernerklæringer beskrives som et viktig middel for å gi informasjon, at erklæringen bør være tilgjengelig direkte på hovedsiden til nettstedet. Slik de er tilgjengeliggjort hos If og Store-

⁷⁰ I denne sammenheng vil jeg allerede her nevne at nesten alt av innhold kan knyttes opp mot informasjonsplikten i pol.§19. På hvilken måte erklæringene kan tolkes i lys av denne bestemmelsen vil drøftes samlet først i kapittel 5.1.

⁷¹ If(2013 a), se vedlegg 1

⁷² Storebrand(2013 a), se vedlegg 2

⁷³ If(2013 b), se vedlegg 3

⁷⁴ WP 43

brand må sies å være i henhold til denne anbefalingen. Videre står det samme sted at lenken må ha en tittel som gjør at internetbrukeren forstår innholdet. For erklæringen som heter "Cookies" kan en stille spørsmål om dette er egnet tittel for slik informasjon. Gjennom økende kunnskapsnivå vil nok også en slik tittel være forståelig, sammenhengen med personvernet er nok derimot mer uklart. De som søker denne informasjonen vil finne den, og det bør nok aksepteres som tittel. Hva cookies er, sammenhengen med personvernet og spørsmål knyttet til informasjon om dette vil drøftes nærmere i kapittel 4.3.

I Datatilsynets rapport om bruken av personvernerklæringer kommer If og Storebrand totalt sett best ut, sammen med nettstedene til Forsvaret og Skandiabanken. Av disse fire hadde brukerne til If og Storebrand lettest tilgang på informasjon. Det kan legges til at tilgjengeligheten for Storebrand også har blitt bedre siden tidspunktet for undersøkelsen til Datatilsynet, erklæringen lå ikke da tilgjengelig fra forsiden.⁷⁵ Tilgjengeligheten medfører at informasjon gis raskt, men forutsetter likevel at brukerne oppsøker informasjonen

4.2 Informasjon om selskapene

I erklæringene under overskriften "*Behandlingsansvarlig*" hos begge selskaper søkes det å informere om hvem som innhenter opplysninger om kundene. I erklæringen til Storebrand informeres det om at i Storebrandkonsernet er det "*det selskapet som er avtalepart mot kunden*" som er behandlingsansvarlig. For forsikringsdelen av virksomheten er dette Storebrand Forsikring AS,⁷⁶ en del av konsernet Storebrand ASA, men dette kommer ikke frem i erklæringen. Brukeren av denne nettsiden vil altså ikke få spesifikk informasjon om hvem som er behandlingsansvarlig. Her ser vi konsekvensen av at Storebrand er en del av et større konsern og at erklæringen er tilpasset ulike typer virksomhet gjennom generell orientering utad. Dette er enklere for If, som gir informasjon om at det er If Skadeforsikring NUF som er behandlingsansvarlig.

⁷⁵ Datatilsynet(2011 a)

⁷⁶ Storebrand(2013 b)

Det er den behandlingsansvarlige som er ansvarlig for at lovens grunnkrav til behandling av personopplysninger oppfylles og etterleves, jfr. pol.§ 11, og at tilstrekkelig informasjonssikkerhet foreligger, jfr.§ 13. Det er også den behandlingsansvarlige som skal svare på henvendelser om informasjon om behandlingen, jfr.§ 16.

Av særlige oppgaver for den behandlingsansvarlige trekker Personvernnemnda frem det å:

*"sørge for informasjonssikkerheten, jf personopplysningsloven § 13, og gi informasjon til de registrerte om formålet med behandlingen, utlevering av opplysninger og retten til å kreve innsyn og retting, jf personopplysningsloven § 19."*⁷⁷

Altså har denne et særlig ansvar for reglene vedrørende informasjon og åpenhet. Begrunnelsen for å informere om behandlingsansvarlig kan sies å være nettopp de forhold som Personvernnemnda her trekker frem. Å få informasjon om behandlingsansvarlig, og med det få vite hvilket selskap som er ansvarlig, vil gi muligheten til å vurdere om selskapet er egnet til å behandle ens opplysninger, også før en gir fra seg opplysninger.

4.3 Hvordan selskapene kommuniserer

4.3.1 Innsamlingen av personopplysninger

Både If og Storebrand har et skjema for innsending av opplysninger på sine nettsider, og er en kanal for overføring av opplysninger. Storebrand informerer i erklæringen om at deres kommunikasjonskanal ovenfor kunder i enkelte tilfeller også går over e-post. Innsending av opplysninger gjennom et nettskjema knyttes direkte til bruk av nettsiden, og en kan da stille krav blant annet til de sikkerhetsløsninger som anvendes, jfr. pol.§ 13. Innsending gjennom e-post kan ikke knyttes til bruk av den konkrete nettsiden, og kan av teknologiske grunner ikke regnes som sikker. Storebrand informerer derfor om at de ikke kan garantere at e-post

⁷⁷ PVN-2007-01

som går gjennom det alminnelige nettet ikke blir kjent for andre. Storebrand sine kunder blir derfor i erklæringen oppfordret til kun å sende sensitive opplysninger inn gjennom innlogging på de personlige sidene.

If informerer om at det tas opptak av telefonsamtaler, og at disse samtalene kan søkes opp ved hjelp av blant annet telefonnummer. Kopi av andre kommunikasjonsformer, som e-post, kan gjenfinnes etter for eksempel kundeidentitet. Brukerne får her konkret informasjon om at deres kommunikasjon kan knyttes direkte til dem som person, og at lagring av denne kommunikasjonen skjer. Noe som ikke nødvendigvis er åpenbart for kunden i et slikt tilfelle. Lagring er behandling av personopplysninger, jfr.§ 2 nr.2, og den registrerte må være informert for å kunne gi et tilstrekkelig samtykke, jfr.§ 2 nr.7, jfr.§ 8. Det foreligger derfor gode grunner til å gi slik informasjon.

4.3.2 Webanalyseverktøy og bruken av informasjonskapsler

If informerer ikke om bruk av informasjonskapsler i erklæringen, men i tilleggskildet kalt "*Cookies*".⁷⁸ Det uttales der at data lagres i informasjonskapsler (cookies) på brukerens datamaskin, og som elektroniske spor på if.no. Gjennom aktivitet på en nettside vil en bruker ofte legge igjen elektroniske spor i form av IP-adresse, bruksmønster, nettleser som benyttes, lokasjon og andre forhold. Slike spor innhentes gjennom bruk av webanalyseverktøy og informasjonskapsler (cookies), og kan være opplysninger som kan knyttes til en enkeltperson, altså være en personopplysning i personopplysningslovens forstand, jfr.§ 2 nr.1.

Hvilke webanalyseverktøy som benyttes får vi ikke vite noe om av If. Storebrand informerer om at de benytter verktøyene Webtrends og Google Analytics,⁷⁹ og Storebrand oppgir at informasjonen som samles inn ikke inneholder "*identifiserbare personlige opplysning-*

⁷⁸ Se vedlegg 3, If(2013 b)

⁷⁹ For mer informasjon om disse verktøyene, se Webanalytiker(2013)

er". Dette må forstås som at Storebrand hevder at personopplysninger ikke samles inn gjennom analyseverktøyet, og at det som samles inn vil falle utenfor området for personopplysningsloven.

If gir omfattende informasjon om hvilke opplysninger som innhentes, blant annet at de:

"innhenter opplysninger om maskinvare og programvare på datamaskinen din, herunder IP-adresse, nettleser og operativsystem, domenenavn, tilgangstider og tilknyttede nettsideadresser."

Som et eksempel på hvordan elektroniske spor kan brukes, uttaler If at det kan hende *"at en av våre kunderådgivere kontakter deg med tilbud hvis du avbryter et kjøp i nettbutikken"*. Dette tyder på at en gjennom et elektronisk spor på nettsiden kan knytte aktivitet tilbake til brukeren. Dette vil nok falle inn under personopplysningsloven, jfr.§ 3, jfr.§ 2 nr.1.

En IP-adresse vil også i mange tilfeller kunne knyttes til en person gjennom maskinvaren som brukes og er da en personopplysning, mens hvilken nettleser som benyttes nok ikke er en personopplysning. Det må derfor trekkes en grense mellom elektroniske spor om en bruker, og elektroniske spor om en bruker som også må anses som personopplysninger. En må falle ned på den alminnelige vurderingen om hvorvidt en opplysning kan knyttes tilbake til en person. Det presiseres i forarbeidene til loven at innsamling av personopplysninger bunner i et ønske om å *"tilegne seg informasjon om den registrerte"*, og derfor ikke omfatter elektroniske spor som er *"nødvendige for å gjennomføre tekniske prosesser og som utelukkende nyttes til dette"*.⁸⁰

Ved innsamling av spor som kan knyttes til en person vil det forekomme behandling av personopplysninger, og personopplysningsloven vil gjelde fullt ut. For andre elektroniske

⁸⁰ Ot.prp.nr.92 (1998-1999) side 119.

spor har EU-direktiv 2009/136/EF (heretter: cookie-direktivet) kommet inn med regulering av bruken, for å sikre et personvern også for slike opplysninger. Området for personvernet er dermed strukket. Slike spor må nok sies å være mer enn bare spor som er nødvendig for tekniske prosesser, men grensen er fin både oppad og nedad. Cookie-direktivet er ikke implementert i Norge per april 2013, men den 1.mars 2013 ble forslag til endring i ekomloven⁸¹ lagt frem, en endringslov som er ment å implementere de nye EU-reglene i cookie-direktivet.⁸²

Det følger av cookie-direktivets art. 21, og som det også fremkommer av lovforslaget,⁸³ at det også for innsamling av elektroniske spor gjennom analyseverktøy vil stilles krav om blant annet en informasjonsplikt som ligner på pol.§ 19. Det er forslag til ny § 2-7B i ekomloven som vil være relevant for vurderingen av innholdet i erklæringene, denne bestemmelsen lyder:

"§ 2-7b Bruk av informasjonskapsler/cookies

Lagring av opplysninger i brukers kommunikasjonsutstyr, eller å skaffe seg adgang til slike, er ikke tillatt uten at brukeren er informert om hvilke opplysninger som behandles, formålet med behandlingen, hvem som behandler opplysningene, og har samtykket til dette. Første punktum er ikke til hinder for teknisk lagring av eller adgang til opplysninger:

- 1. utelukkende for det formål å overføre kommunikasjon i et elektronisk kommunikasjonsnett*
- 2. som er nødvendig for å levere en informasjonssamfunnstjeneste etter brukerens uttrykkelige forespørsel"*

⁸¹ Lov om elektronisk kommunikasjon nr.83 av 04.07.2003

⁸² Prop.69 L (2012-2013)

⁸³ Prop.69 L (2012-2013) side 102.

Hensynet bak bestemmelsen er å sikre brukernes personvern, og tanken om at også elektroniske spor bør underlegges et slikt vern⁸⁴ selv om de ikke alltid vil falle inn under personopplysningsbegrepet slik pol.§ 2 nr.1 oppstiller det.

At Storebrand uttaler at deres webanalyseverktøy ikke samler inn personopplysninger er en dristig uttalelse. Storebrand benytter Google Analytics (heretter: GA), og spørsmålet om det er slik at GA samler inn personopplysninger gjennom deres tilgang på IP-adresser har vært oppe til vurdering hos Datatilsynet. Dette i forbindelse med at både Skatteetaten og Lånekassen benytter GA på sine nettsider. Datatilsynet uttalte i forbindelse med denne saken at når en virksomhet benytter seg av webanalyseverktøy vil det være avgjørende at de kjenner til dette selskapets håndtering av innsamlet materiale, og om opplysninger vil være underlagt personopplysningsloven. Det er den enkelte virksomhet som har ansvaret for at databehandleren for webanalyseverktøyet holder seg innenfor personopplysningsloven, og databehandleravtale må foreligge dersom virksomheten har satt ut deler av sin behandling til andre, jfr. pol.§ 15.

Det fremsto for Datatilsynet som uklart hvorvidt de offentlige etatene kjente til GA's bruk av IP-adresser, og de ble bedt om å klarlegge dette spørsmålet.⁸⁵ Etter at etatene innhentet informasjon fra GA, og Datatilsynet utførte egne vurderinger, kom det frem at GA anonymiserer IP-adressene på et så tidlig stadium at det ikke kan oppfattes som behandling av personopplysninger, og at de kun benyttes til analyseformål. Datatilsynet fattet derfor vedtak om at etatene hadde tilstrekkelig informasjon om GA's behandling av IP-adresser.⁸⁶ IP-adressene kan i dette tilfellet nok ikke knyttes tilbake til person, men spørsmålet fremstår fortsatt som noe uavklart, i og med at IP-adressene faktisk samles inn. Det er nå akseptert

⁸⁴ Prop.69 L (2012-2013) side 102.

⁸⁵ Datatilsynet(2013 b)

⁸⁶ Datatilsynet(2013 c)

av Datatilsynet at offentlige etater benytter GA, likevel forutsatt en tilstrekkelig databehandleravtale.⁸⁷

Da vi ikke kjenner til hvilket analyseverktøy If benytter vil vi ikke umiddelbart kunne si noe om hvordan IP-adresser behandles av If sine databehandlere. Hvilke webanalyseverktøy som benyttes er noe en bør informere om, ifølge både Datatilsynet⁸⁸ og Artikkel 29-gruppen. Å informere om informasjonskapsler i personvernerklæringen vil i følge Artikkel 29-gruppen bidra til informasjonssikkerhet og kunnskap, og slik medvirke til å hindre at de medfører en risiko. Artikkel 29-gruppen uttaler dette slik:

*"considers that first party analytics cookies are not likely to create a privacy risk when they are strictly limited to first party aggregated statistical purposes and when they are used by websites that already provide clear information about these cookies in their privacy policy as well as adequate privacy safeguards."*⁸⁹

Som vi ser anføres det av Storebrand at det ikke samles inn slike personopplysninger, mens det hos If kan tyde på at elektroniske spor innhentet ved analyse kan knyttes til person og således er underlagt personopplysningsloven. Uansett ser en verdien av informasjon også om behandlingen av opplysninger som ikke nødvendigvis er en personopplysning, samtidig som det er viktig at de enkelte virksomheter har en god databehandleravtale og kjenner til de enkelte databehandlers praksis. Kunnskapen om informasjonskapsler og hva dette er og brukes til er fortsatt lav, og det vil derfor være særlig praktisk med god informasjon om dette utad.

⁸⁷ Datatilsynet(2013 c)

⁸⁸ Datatilsynet(2012 d)

⁸⁹ WP 194

4.3.3 Mottakeren av informasjonen

Gjennom informasjonen som gis, forstår en at erklæringen til Storebrand gjelder for konsernet Storebrand, ikke kun forsikringsvirksomheten. Erklæringen er derfor ikke tilpasset de ulike kunder de ulike selskapene i konsernet har. For de ulike kundetyper vil forhold som hvem som er behandlingsansvarlig, formål og lignende kunne være ulikt, og det kunne tenkes at dette ville påvirket innholdet i erklæringen, jfr. de ulike krav som følger særlig av pol.§ 8 og § 11. For If er ikke dette en aktuell problemstilling.

En mottaker av en erklæring vil være både brukeren av nettstedet, og den enkelte kunde. If har delt opp informasjonen etter de to, avhengig av type mottaker, og "Cookies"-erklæringen retter seg utelukkende til brukerne av nettstedet. Den samme informasjonen som vi hos If finner i erklæringen kalt "*Cookies*", finner vi igjen i erklæringen til Storebrand sammen med den generelle personverninformasjonen. Selv om Storebrand anfører at webanalyseverktøyet ikke samler inn opplysninger, er det klart at også brukere av nettsiden til Storebrand kan gi fra seg personopplysninger. Storebrand har likevel valgt å ikke skille mellom ulike typer lesere, og erklæringen er den samme både for kunder av selskapene, og for de som er brukere av nettsiden.⁹⁰

Datatilsynets egen praksis på området er interessant. De har i likhet med If to erklæringer; den ene en generell personvernerklæring om tilsynets behandling,⁹¹ og den andre en spesiell personvernerklæring for besøkende av nettsiden datatilsynet.no.⁹² Altså skiller de mellom typer lesere, i likhet med If. En grunn til å skille mellom informasjonen vil være at innsamlingen kan forekomme på ulike måter, og selv om en bruker og en kunde kan være samme person vil erklæringene fremstå som mer tilpasset og en finner kanskje fortere frem til akkurat den informasjonen en søker. Temaet vil drøftes i videre i kapittel 5.2.3.

⁹⁰ Jeg minner om at dette kan være samme person.

⁹¹ Datatilsynet(2012 b)

⁹² Datatilsynet(2012 c)

4.4 Informasjon om selskapenes behandling av personopplysninger

4.4.1 Hvilke opplysninger samles inn

Begge virksomheter har i sine personvernerklæringer et punkt som heter "*Innhenting av personopplysninger*". If informerer om at personopplysninger samles inn, og at disse hentes fra "*kunden selv, representanter for kunden, kredittinformasjonsregistre og offentlige registre*". Storebrand informerer om at opplysninger hentes fra kunden, og fra offentlige eller private institusjoner. Kundene gis altså her informasjon i forkant om at opplysninger kan innhentes, også fra andre.

Gjennom teksten i personvernerklæringen får brukerne helt klart vite at If og Storebrand kan innhente personopplysninger gjennom deres virksomhet, men det gis lite konkret informasjon om hva som innhentes. Ett konkret eksempel som derimot gis er om innsamling av helseopplysninger, som If informerer om. Helseopplysninger er sensitive opplysninger, slik at behandlingen av disse krever særskilt behandlingsgrunnlag, jfr. pol.§ 2 nr.8, jfr.§ 9.

Gjennom eksemplene brukt av If om hvem opplysninger innhentes fra, får brukerne likevel en innsikt i hva slags opplysninger som kan bli samlet inn, nemlig kredittinformasjon og offentlig registrerte opplysninger. Storebrand er her litt mindre presis om de situasjoner der de henter informasjon fra andre enn kunden, og ingen eksempler gis utenom "*institusjoner*". Det gis videre av Storebrand opplysning om at:

"Du vil bli informert dersom vi innhenter opplysninger om deg, med mindre innsamlingen er lovbestemt, varsling er umulig eller uforholdsmessig vanskelig eller det er på det rene at du allerede kjenner til de opplysningene varselet skal inneholde".

Denne setningen refererer til reglene i pol.§ 20(1) og (2). Det kan nok ikke forventes at det gis informasjon om hva som samles inn i en slik erklæring. Ved innsamling "*fra den registrerte selv*", jfr. pol.§ 19(1), vil en virksomhet heller ikke ha en lovpålagt plikt til å informere om nøyaktig *hvilke* og *hva slags* opplysninger som samles inn. Den registrerte antas da å

vite hvilken informasjon han gir fra seg. Det er imidlertid foreslått at dette bør inkluderes i en slik erklæring, jfr. NOU 2009:1.⁹³ Dette problematiseres nærmere i kapittel 5.2.3.

4.4.2 Formålet med behandlingen

If opplyser i erklæringen at deres konsesjon for behandling av personopplysninger omfatter formålene "*kundeadministrasjon, fakturering og gjennomføring av forsikringsavtaler*". Storebrand orienterer at de har konsesjon for de samme forhold, men også for andre: markedsføring og kundeoppfølging, risikoklassifisering av kunder og kredittporteføljer, og forebygging og avdekking av straffbare handlinger. Altså har de, gitt informasjonen i erklæringen, en videre konsesjon enn If. Enkelte av disse formål må nok sees på bakgrunn av Storebrand sin utvidede virksomhet i forhold til If.

Personopplysninger skal bare "*nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet*", jfr. pol.§ 11(1) bokstav b. Forsikringsvirksomhet er konsesjonspliktig, jfr. pof.§ 7-2, noe som innebærer at Datatilsynet har foretatt den interessevurdering som må gjøres om formålet er "*saklig begrunnet*" før behandling kan foretas, jfr. pol.§ 11(1) bokstav b, jfr.§ 34. Selskapene har derfor frihet innenfor konsesjonens fastlagte formål, som etter den standardiserte konsesjonen for forsikringsvirksomhet og pof.§ 7-2 er: "*kundeadministrasjon, fakturering og gjennomføring av forsikringsavtaler*" i tråd med gjeldende regelverk.⁹⁴ Datatilsynet har vurdert disse formål som forenelige med personopplysningsloven og personvernprinsippene.

En ser at informasjonen som gis av If og Storebrand tilsvarer konsesjonen. De aktuelle virksomheter skriver også noe mer om formålet i erklæringene. If informerer om at personopplysninger som innhentes er nødvendig for å kunne "*administrere forsikringer, oppfylle selskapets avtaleforpliktelser og for øvrig kundenes ønsker*". Dette er i tråd med de konse-

⁹³ NOU 2009:1 side 124.

⁹⁴ Datatilsynet(2011 b)

sjonerte formål, men gir noe mer innsyn i hva opplysningene brukes til. Videre opplyses det at opplysningene vil kunne benyttes for å vurdere innhold og vilkår i forsikringene, samt til markedsanalyse og markedsføring, og gi kunden informasjon om selskapets tjenester forøvrig. Denne posten kan muligens forstås på bakgrunn av pol.§ 21, som tar for seg informasjonsplikter ved sammenstilling av personprofiler. En slik profil kan blant annet benyttes for å rette markedsføring dit en har fått kjennskap gjennom profilen at det kan foreligge en interesse, for eksempel gjennom en antagelse om preferanser.⁹⁵

Men også i konsesjonen finnes regler om formålet markedsføring. Det sies her at:

*"Bruk av opplysninger til et annet formål innen samme selskap/konsern og overføring av opplysninger til andre selskaper krever den registrertes samtykke med mindre annet følger av personopplysningsloven §§ 8 (...) Datatilsynet finner å akseptere at registrering i felles konsernkunderegister med formålet administrasjon, kundepleie, herunder markedsføring, kan skje med hjemmel i personopplysningsloven § 8 bokstav f, jf. § 12. Under forutsetning av at opplysningstypene begrenser seg til kontaktopplysninger, fødselsnummer, selskapstilhørighet og produkttype."*⁹⁶

Markedsføring er derfor godkjent som et tilleggsformål.

Storebrand formidler at det er personopplysningsloven og konsesjonen fra Datatilsynet som regulerer bruken av personopplysninger. Det uttales videre at opplysningene i all hovedsak brukes til å følge opp kundene, herunder å informere kundene om de produktene de har hos Storebrand. Til sammenligning, der If informerer generelt om at opplysningene kan benyttes til markedsføring, skiller Storebrand mellom nøytrale opplysninger, og opplysninger som ikke er nøytrale. Nøytrale kan brukes til informasjon om produkter og tjenester hos Storebrand. De som ikke er nøytrale kan kun benyttes dersom det foreligger et samtykke.

⁹⁵ Schartum(2012) note 98.

⁹⁶ Datatilsynet(2011 b)

Slikt samtykke kan gis gjennom kundens personlige side på nettstedet, såfremt det tilfredsstiller kravene til samtykke i pol.§ 2 nr.7: samtykket må være frivillig, uttrykkelig og informert. Det er klart at elektronisk samtykke er gyldig i formen, jfr. uttalelse i sak for Personvernemnda.⁹⁷

Personopplysningsloven oppstiller ikke et skille mellom nøytrale og ikke-nøytrale opplysninger, men dette gjøres i personopplysningskonsesjonen for finansvirksomhet. Avsnittet hos Storebrand knytter seg således til denne konsesjonen, der det uttales om slike opplysninger:

*"Følgende opplysninger er i konsesjonen angitt som nøytrale: Kundens navn, kontaktopplysninger (så som postadresse, telefonnumre og e-postadresse), fødselsdato og hvilke tjenester eller produkter kunden har inngått avtale om. Banken kan, uten kundens samtykke, benytte slike nøytrale personopplysninger til markedsføring og kundeoppfølging overfor egne kunder og kunder i andre foretak i samme konsern/konserngruppe som banken. Slik bruk av nøytrale opplysninger gjelder uavhengig av om tjenesten eller produktet som tilbys faller innenfor en produktkategori hvor det allerede foreligger et avtaleforhold mellom kunden og banken."*⁹⁸

I siste setning slås det altså fast at slike opplysninger også kan benyttes om og mot kunder utenfor finansvirksomheten, så lenge det er innenfor konserndriften. Derfor vil dette også gjelde ovenfor forsikringskundene. I motsetning til tidligere ser en her en fordel ved at erklæringen retter seg mot hele konsernets kundegruppe.

⁹⁷ PVN-2004-08

⁹⁸ Datatilsynet(2005)

4.4.3 Utlevering

4.4.3.1 Deling med underleverandører

I erklæringen til If står det at personopplysninger kan utleveres til selskap og organisasjoner If samarbeider med, både innenfor og utenfor EØS- og EU-området. Storebrand informerer i avsnittet med tittel "*Slik videreformidler vi personopplysninger*", at de har taushetsplikt om kundeopplysninger, med mindre kunden samtykker eller Storebrand er forpliktet ved lov til overlevering. Storebrand gir noe mer informasjon enn If om delingen til samarbeidsparter. En får i deres erklæring vite at underleverandører vil kunne ha behov for opplysninger, men at dette ikke regnes som utlevering fordi det reguleres av databehandleravtaler mellom partene. Det bekreftes videre at underleverandører kun benytter opplysninger til de samme formål som de er innhentet for.

En databehandleravtale er en avtale mellom den behandlingsansvarlige, og en som behandler opplysninger på dennes vegne, en databehandler, jfr. pol.§ 15. Dersom en ikke har en databehandleravtale vil deling med underleverandører kreve at de generelle vilkår for behandling av personopplysninger er til stede. På den annen side medfører en databehandleravtale at databehandleren er underlagt de begrensninger som påhviler den behandlingsansvarlige, og kan ikke gå utenfor dennes behandlingsrammer. Samtidig er det fortsatt den behandlingsansvarlige som har det fulle ansvaret, dette slipper en ikke unna gjennom databehandleravtalen.⁹⁹

Innen de formål virksomheten har konsesjon for kan personopplysninger deles og utleveres, noe som indirekte følger av pol.§ 15. Etter pol.§ 8 bokstav f kan utlevering skje dersom det er nødvendig og den det "*utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen*". Det behøves da ikke å innhentes samtykke. Nettopp derfor vil slik informasjon være verdifull for opprinnelig sam-

⁹⁹ Johansen(2001) side 136.

tykke. Dette er kunnskap en alminnelig person nok ikke sitter med, og erklæringene er god kilde til informasjon.

4.4.3.2 Deling som følge av lov

If informerer i erklæringen om at opplysninger utleveres til fellesregistrene for forsikringsbransjen: ROFF og FOSS. Det gis også informasjon om formålet med registrene, og brukerne får slik vite hvorfor opplysningene deles med disse. Tillatelse til utlevering av opplysninger til disse registre følger av konsesjonen.¹⁰⁰ Storebrand har ikke med informasjon om disse registrene, selv om en kan anta at også Storebrand deler informasjon med dem.

Slik deling må anses som utlevering med hjemmel i lovgivning. Begge virksomheter oppgir videre at der det foreligger en opplysningsplikt overfor offentlig myndighet, vil opplysninger bli overlevert i henhold til myndighetenes krav, og uten kundens samtykke. Når formidling av opplysninger uttrykkelig er fastsatt i lov, foreligger for eksempel ikke informasjonsplikt etter § 20(2), jfr.(1) siste setning. Hvorvidt en må opplyse om deling som følge av lov varierer med grunnlaget, og en kan kanskje anføre at dette heller ikke alltid er informasjon som er helt egnet for en personvernerklæring.

4.4.3.3 Konsernutfordringer og overføringer til utlandet

Under overskriften "*Konsernsamtykke*" opplyser Storebrand om at deres kunder kan gi et såkalt konsernsamtykke inne på den personlige siden til kunden på nettstedet. Det opplyses om at et slikt samtykke innebærer at opplysningene om kundene blir tilgjengelig for alle selskapene i Storebrandkonsernet. Dette for at Storebrand skal "*kunne gi deg best mulig kundeservice, samt informasjon og tilbud om de produkter og tjenester vi tilbyr*", og at de da kan sørge "*for at rådgivning og tilbud er bedre tilpasset*" kundens behov. Lenger ned i erklæringen gis det informasjon om et felles konsernregister tilgjengelig for alle konsern-

¹⁰⁰ Datatilsynet(2011 b)

selskapene, og det uttalte formålet er å oppnå størst mulig samordning av tilbudet av tjenester og rådgivning fra de forskjellige selskapene. Dersom registeret skal inkludere opplysninger utover nøytrale opplysninger kreves det samtykke. Dette sies et helt annet sted enn avsnittet om konsernsamtykke, selv om det gjelder de samme forhold. Dette er egnet til å villede kundene til å gi samtykke til videre bruk av opplysninger enn bare det å sette nøytrale opplysninger inn i et konsernregister.

Storebrand er et nordisk konsern med datterselskaper i flere nordiske land, og delingen innen konsernet kan medføre at opplysninger flyttes ut av Norge. If opplyser som nevnt at også de kan finne på å dele opplysninger, både innenfor og utenfor EU- og EØS-land. Dersom en deler personopplysninger med andre underselskaper innenfor grensen vil en falle ned på de generelle vilkår for behandling og krav til databehandleravtale. Overføring til utlandet medfører derimot tilleggskrav, jfr. pol.§ 29 og § 30.

Som hovedregel kan personopplysninger bare overføres til stater som sikrer en forsvarlig behandling av opplysningene, jfr.§ 29(1). Det følger av samme ledd at de stater som har gjennomført personverndirektivet anses som forsvarlige. Ved overføring innen de nordiske land anses dermed tilleggskravet oppfylt. Gjennom å sikre seg et samtykke fra sine kunder vil Storebrand også kunne overføre til stater som ikke anses å sikre forsvarlig behandling, jfr.§ 30(1) bokstav a. Dette er først og fremst stater utenfor EU og EØS, og for amerikanske bedrifter som ikke har inngått en Safe Harbor-avtale.¹⁰¹ Kravene til samtykke er slik som Storebrand skriver, det må være "*frivillig, uttrykkelig og informert*", jfr. pol.§ 2 nr.7. Innholdet i disse vilkår vil variere etter hva en gir samtykke til, og det må antas at ved overføring til stater som ikke er godkjent vil informasjonskravet være vesentlig. Dersom samtykket skal være gyldig må det gis videre informasjon på de personlige sidene på nettstedet det henvises til for informasjon, enn det som er gitt i personvernerklæringen.

¹⁰¹ Amerikanske virksomheter kan slutte seg til et sett av Safe Harbor-prinsipper, og overføring av personopplysninger dit vil da anses forsvarlig, se Datatilsynet(2011 e) og Datatilsynet(2011 c)

Et alternativ for overføring til utlandet er å stille garanti godkjent av Datatilsynet, jfr. § 30(2). En slik garanti vil kunne være å bruke en standardavtale, for eksempel EU sin,¹⁰² men særlig praktisk for store konsern vil være å inngå såkalte bindende konsernregler (Binding corporate rules). Artikkel 29-gruppen har utarbeidet veiledere for inngåelsen av slike regler,¹⁰³ og Datatilsynet antas å godkjenne slike garantisøknader dersom de følger disse standardene.¹⁰⁴ Verken Storebrand eller If har per i dag inngått en slik, men ved omfattende utlevering over landegrenser er denne ordningen svært aktuell.

4.4.4 Frivillighet

Storebrand informerer om at en vil bli informert om innsamling, med mindre dette er lovbestemt. Få konkrete situasjoner nevnes, og ingen eventuelle hjemler nevnes. Det uttales at nøytrale kundeopplysninger "*kan brukes som*" grunnlag for markedsføring. Dette forstås som at dette ikke er frivillig, og som nevnt følger dette av at markedsføring er godkjent formål i konsesjonen.

I neste avsnitt hos Storebrand heter det at:

"Bruk av opplysninger som ikke er nøytrale, for eksempel transaksjonsopplysninger og andre dybdeopplysninger om kundeforholdet og bruk av tjenestene kan bare brukes i markedsføringsøyemed dersom det foreligger et frivillig, informert og uttrykkelig samtykke fra deg som kunde. Slikt samtykke kan du gi på dine personlige sider."

¹⁰² Datatilsynet(2011 d)

¹⁰³ WP 153

¹⁰⁴ Datatilsynet(2011 c)

For opplysninger som går utover nøytrale vil det derimot kreves tilleggssamtykke. Dette følger opp vilkår i Storebrands tilleggskonsesjon for finansvirksomhet, hvor det uttales:

*"Dersom banken i markedsføringsøyemed utarbeider en personprofil om kunden og bruker opplysninger utover de nøytrale i denne sammenheng, skal det foreligge et behandlingsgrunnlag som nevnt i personopplysningslovens § 8. Kunden skal informeres, i samsvar med kravene i personopplysningslovens § 21, når personprofilen benyttes. Informasjonsplikten gjelder også når profilen er utarbeidet kun på bakgrunn av nøytrale personopplysninger."*¹⁰⁵

If informerer spesifikt om at dersom de samler inn helseopplysninger vil disse behandles med varsomhet, og samtykke vil alltid innhentes. Helseopplysninger er sensitive opplysninger, jfr. pol.§ 2 nr.8 bokstav c, og behandlingsgrunnlaget er her både konsesjonen og samtykke: frivillighet. If gir lite informasjon om frivillighet og innhenting av samtykke i sin erklæring. Heller ikke i forbindelse med informasjon om innsamling fra andre enn den registrerte selv, gis slik informasjon.

Det er selvfølgelig frivillig å inngå en forsikringsavtale, men når den er inngått vil konsesjonen kunne avgjøre behandlingsgrunnlaget uten at videre samtykke innhentes. Samtykke og frivillighet er som nevnt grunnleggende prinsipper innen personvern, og samtykke er hovedgrunnlag for gyldig behandling, jfr. pol.§ 8(1).

Det er enkelte opplysninger forsikringsselskaper kan behøve å samle inn, hvor lovgivning er grunnlaget. Ett eksempel er innhenting av kredittinformasjon, hvor samtykke ikke er like praktisk. If har med at de kan hente inn opplysninger fra kredittinformasjonsregistre, men det uttales ikke at dette ikke er frivillig.

¹⁰⁵ Datatilsynet(2005)

For forsikringsvirksomhet generelt, og for de opplysninger de typisk benytter i utøvelsen av forsikringsavtalen, vil det naturlig nok ofte være samtykke som er behandlingsgrunnlaget. Slikt samtykke innhentes først og fremst gjennom forsikringsavtalen, men også elektronisk gjennom nettsiden. Slik vi så i kapittel 4.4.3 kan det for eksempel gis konsernsamtykke gjennom innlogging på nettsiden til Storebrand, og informasjonen i erklæringen er svært praktisk.

4.5 Informasjon om rettigheter

Overfor er flere av pliktene som er pålagt virksomheter etter personopplysningsloven drøftet. Personopplysningsloven har som nevnt også regler presentert som rettigheter for brukerne, og begge virksomheter gir til dels omfattende informasjon på dette området. Storebrand gjør det først og fremst gjennom et avsnitt som heter "*Dine rettigheter*" hvor det gis informasjon om temaene innsyn og retting/sletting, og If har et avsnitt som heter "*Innsyn og retting*".

4.5.1 Lagring, sletting og retting

Storebrand informerer om at kundenes opplysninger blant annet lagres i et kunderegister for Storebrandkonsernet, og i ulike saksbehandlingssystemer. De gir begrunnelse både for hvorfor lagring skjer, og for hvor lenge de har mulighet til å lagre opplysningene.

"Opplysningene lagres så lenge det er nødvendig for å oppfylle formålet med behandlingen. Det vil i praksis si så lenge avtaleforholdet eksisterer. Dersom avtalen sies opp, vil Storebrand på grunn av muligheten for fremtidige erstatningskrav som kan tilbakeføres til avtaleforholdet, lagre opplysningene frem til foreldelsesfristen for de aktuelle produktene er utløpt."

If har en enklere tilnærming til det å informere om lagring, og skriver at:

"I henhold til personopplysningslovens § 28 skal opplysninger som ikke lenger er nødvendig ut fra det formål de er lagret for slettes. If lagrer personopplysninger om kunder i henhold til den enhver tid gjeldende lovgivning".

Altså får ikke brukerne til If noen innsikt i hvorfor, eller for hvor lenge, slik de gjør i større grad i teksten til Storebrand. Hva som ligger i *"enhver tid gjeldende lovgivning"* er ikke nødvendigvis åpenbart for en alminnelig bruker av nettsiden eller kunde av If. Heller ikke er det åpenbart hvor lenge det er nødvendig å oppbevare opplysninger. Både If og Storebrand gjør relativt kort rede for reglene, og det henvises til aktuell lovbestemmelse, pol.§ 28.

Også konsesjonen oppstiller noen vilkår for lagring utover loven. For forsikringsvirksomhet følger det av konsesjonen at opplysningene må slettes senest etter 10 år.¹⁰⁶ Verken If eller Storebrand gir altså fullstendig informasjon om forhold rundt lagringen av personopplysninger.

If sier i erklæringen at en kan kreve rettet opplysninger som *"ikke er riktige eller de er ufullstendige"*, mens Storebrand sier at en kan kreve rettet opplysninger som er *"mangelfulle eller unødvendige"*. Pol.§ 27 hjemler retten til å kreve retting, en bestemmelse som følger opp lovens formål, jfr.§ 1(2) om *"tilstrekkelig kvalitet på opplysningene"*. If sin ordlyd er nærmere lovens ord, men også Storebrand får frem regelen og hensikten bak. Ved å ta med begrepet *"unødvendige"* opplysninger får også Storebrand frem at en vil ha en rett til å få fjernet opplysninger som selskapet ikke har behov for. Slik informasjon som her gis er viktig for at brukerne og kundene får den kunnskapen de behøver for å være i stand til å benytte sine egne rettigheter.

¹⁰⁶ Datatilsynet(2011 b)

4.5.2 Innsynsrett

Det opplyses i begge erklæringer at kunden har rett til å få informasjon om hva som er lagret. Hos If får en vite at en kan få innsyn gjennom å sende skriftlig henvendelse til If, og at den må være signert. Hos Storebrand uttales det at kunder kan ta kontakt med kunde- og personvernombudet på e-post med spørsmål om behandlingen av personopplysninger.

For å oppfylle innsynsregelen i pol.§ 18 vil poenget være å informere om at både allmennheten og registrerte har rett på innsyn, og informasjon om hvordan dette kan kreves. Ikke å ta med den informasjon som det kan kreves innsyn i, for eksempel "*hvilke opplysninger om den registrerte som behandles*", jfr.§ 18(2). På den annen side, selv om innsyn er noe som i utgangspunktet må kreves, vil slik informasjon kunne være særlig praktisk å ta med i en personvernerklæring. Å gi informasjon i en erklæring vil åpne for at en som søker informasjon får all den info han har behov for allerede gjennom erklæringen, og sparer virksomheten for ressurser knyttet til krav om innsyn.

For allmennheten vil tilgangen på en personvernerklæring være en måte virksomheter viser åpenhet på, og kanskje oppnår tillitt som bedrift. Allmennhetens innsynsrett, jfr.§ 18(1), er relativt vid, og må sies å representere hensynet om åpenhet om personvernhandling. Dette kan underbygge at en virksomhet kan se seg tjent med å informere om slike forhold allerede i erklæringen.

For kunder og brukere som vil ha kontakt med Storebrand er e-posten inntatt i erklæringen, og det er lett å fremsette krav. If gir imidlertid ingen opplysning om hvor en kan sende den skriftlige henvendelsen. Dette er noe Datatilsynet kritiserte i deres analyserapport.¹⁰⁷

¹⁰⁷ Datatilsynet(2011 a)

4.5.3 Andre rettigheter

Storebrand gir nesten for hvert avsnitt i erklæringen forklaringer på hvorfor informasjon gis, hvorfor behandling forekommer og hva som er bakgrunnen for innsamling. If er noe mer reservert, og bruker i det store og hele lovens egne ord, uten videre forklaring. Imidlertid innledes hele erklæringen til If med en redegjørelse av hva en personopplysning er, og hva som menes med behandling av personopplysninger. Dette kan sies å være viktig for forståelsen av innholdet.

Storebrand innleder sin erklæring med informasjon om selskapets personvernombud. Ordningen med et slikt ombud har hjemmel i pof.§ 7-12, og innebærer at en virksomhet frivillig har et ombud som kan hjelpe med å sikre etterlevelse av personvernlovgivningen. Personvernombud er noe If ikke informerer om, og for kunder av If opplyses ingen annen måte enn gjennom skriftlig brev som kontaktmåte med selskapet. Adresse opplyses for øvrig heller ikke om, slik at en må oppsøke andre deler av nettsiden for å få denne informasjonen.

Det er likevel slik at også If har et personvernombud,¹⁰⁸ noe de med fordel kunne inntatt informasjon om i erklæringen. Som Storebrand skriver kan ombudet også være en "*ressursperson for deg som kunde*", og erklæringen er egnet sted for informasjon om dette. En kan anføre at det er nettopp informasjon som kan være en ressurs for brukerne av nettstedet, og kunder av virksomheten, som bør tas med i en erklæring. I analysen til Datatilsynet fikk begge virksomheter trekk i poeng på grunn av at de ikke hadde et personvernombud, og herunder derfor heller ikke informerte om det.¹⁰⁹ Begge virksomheter ville kommet enda bedre ut nå, selv om If fortsatt ikke informerer om tjenesten.

¹⁰⁸ Datatilsynet(2013 a)

¹⁰⁹ Datatilsynet(2011 a)

Av annen informasjon som gis uttaler Storebrand litt om deres plikter som behandlingsansvarlig, blant annet at de må behandle opplysninger på en forsiktig måte, at de har taushetsplikt om kundeopplysninger og at de aldri vil be om sensitiv informasjon i e-postkommunikasjon. Begge selskaper har med lenker i erklæringen til videre informasjon. Hos If gjøres dette gjennom lenke til Datatilsynets nettsider, og til lovdatas nettsider, både til loven og til forskriften, mens det hos Storebrand kun vises til intern informasjon enten gjennom personvernombudet eller lenke til de personlige sidene på nettstedet.

Virksomheter bør foreta en individuell vurdering av sin behandling, og herunder aktivt vurdere de registrertes behov for informasjon.¹¹⁰ Vi ser at både If og Storebrand gir til dels omfattende informasjon om personopplysningsvern, og brukeren gis muligheten til å sette rettighetene sine inn i en sammenheng og slik få forståelse for vernet av egne opplysninger.

4.6 Andre forhold som er tatt med i erklæringen

4.6.1 Ansvar

Storebrand, som eneste av de to, har i erklæringen et avsnitt om ansvar ved feil, mangler og tilgjengelighet. De skriver at de anser informasjonen som gis på sine internettsider som pålitelige, men fraskriver seg videre "*ethvert ansvar*" for feil, mangler og tilgjengelighet. Ansvarsfraskrivelsen knytter seg ikke kun til personvernerklæringen, og fremstår for en alminnelig leser som å gjelde all informasjon som gis av selskapet.

For det første har en slik ansvarsfraskrivelse ingen hjemmel i personopplysningsloven, og loven må forstås preseptorisk i denne sammenheng. En virksomhet som bryter personvernlovgivningen kan ilegges overtredelsesgebyr, jfr. pol.§ 46. Dette kan en ikke fraskrive seg gjennom en slik erklæring.

¹¹⁰ Schartum(2012) note 92

En kan for det andre drøfte konsekvensen av at dette er inntatt i et dokument som heter "*personvernerklæring*". For brukere som søker informasjon om personvern vil teksten være tilgjengelig, men for andre vil informasjonen være "skjult" i et dokument under et annet navn enn det de søker etter.

For det tredje vil ansvarsfraskrivelsen være et bidrag i diskusjonen rundt en erklæring som et avtaledokument, og om en erklæring kan være rettslig bindende. En slik ansvarsfraskrivelse vil vanskelig kunne stå seg i en avtale mellom en forbruker og en bedrift. I forbindelse med at vi står overfor et publisert, skriftlig dokument rettet mot kunder og brukere, kan det også diskuteres hvorvidt denne fraskrivelsen vil kunne stå seg dersom en kunde havner i en konflikt på grunn av en feil virksomheten alene har ansvar for. Dette er problemstillinger utover personvernets grenser, og vil ikke følges videre. Det kan kort nevnes at en personvernerklæring nok er et for uklart konsept, og med et innhold som presenteres på en måte som nok etter norsk rett ikke kan medføre binding. En personvernerklæring kan ikke sees på som en kontrakt selv om likhetstrekk forekommer, men må rett og slett sees på som en uttalelse om virksomhetens etterlevelse av rettsregler som oppfyller reglene om innsyn, informasjon og åpenhet. Dersom det forekommer brudd på loven bør nok dette gå gjennom personopplysningsloven, ikke på bakgrunn av avtalerett.

4.6.2 Immaterialrett og markedsføringsrett

Det gis i erklæringene også informasjon om forhold som går utover rettsområdet personvern. If har inntatt informasjon om muligheten til å reservere seg mot markedsføring fra If, og henviser til markedsføringsloven § 12. Markedsføring er for øvrig også en del av akseptert tilleggsformål ved forsikringsvirksomhet, jfr. konsesjonen,¹¹¹ slik at dette ikke helt er frakoblet personvernet. Storebrand har inntatt et avsnitt om at de har alle immaterielle rettigheter til nettsidene, og at uautorisert bruk av nettsidene ikke er tillatt.

¹¹¹ Datatilsynet(2011 b)

Her kommer annen særlovgivning inn, og påvirker innholdet i erklæringen. Det kan kort nevnes at det kanskje ikke er helt heldig å ta med slik informasjon under overskriften "*Informasjon om behandling av personopplysninger*" eller lignende, det dreier seg ikke om personvern i det hele tatt. Ønsket mottaker for innholdet vil ikke så lett finne informasjonen, og dersom erklæringene inneholder for mye tekst vil en risikere at ingen leser dem. Det vil likevel være viktig å merke seg at også annen informasjon kan finne på å tas med i slike erklæringer. Dette kan nok ikke anbefales som praksis.

5 I hvilken grad er personvernerklæringer hensiktsmessige?

5.1 Gis brukerne og kundene til If og Storebrand hensiktsmessig informasjon i erklæringene?

5.1.1 Premiss for vurderingen

Ovenfor har jeg søkt å svare på hvordan innholdet i erklæringene kan knyttes opp mot personvernlovgivningen. Jeg vil i det følgende komme med noen bemerkninger til om Ifs og Storebrands kunder og brukere faktisk får den informasjonen de behøver for å kunne verne egne personopplysninger gjennom erklæringen.

For at en personvernerklæring skal være hensiktsmessig, kan en si at den informasjonen som gis må være tilstrekkelig til at leserne opplever et vern mot krenkelse, jfr. pol.§ 1(1), og gis informasjon i slik grad at en føler at en er satt i stand til å "*bruke sine rettigheter*".¹¹²

Store deler av innholdet i erklæringene kan særlig knyttes til bestemmelsene i personopplysningslovens kapittel 3 om informasjon og innsyn i behandlingen av personopplysninger. De ulike deler av loven som trekkes frem kan i stor grad finnes igjen i § 19, som slike forhold det skal informeres om. Dette er den samme bestemmelsen som trekkes frem som en del av begrunnelsen for selve bruken av erklæringer, både av Datatilsynet og av Artikkel 29-gruppen.¹¹³ Formålet med § 19 er å gi tilstrekkelig informasjon til registrerte, slik at de kan ta et informert valg om behandling, og blir satt i stand til å verne egne personopplysninger.¹¹⁴ Bestemmelsen fremstår dermed som et utgangspunkt for en drøftelse av erklæringenes hensiktsmessige og informative karakter.

¹¹² Pol.§ 19(1) bokstav e.

¹¹³ Da gjennom henvisning til den tilsvarende artikkel i personverndirektivet, artikkel 10.

¹¹⁴ Ot.prp.nr.92 (1998-1999)

En særlig utfordring med å direkte benytte lovens vilkår på erklæringene oppstår ved at kravene i personopplysningsloven i stor grad gjelder for hver enkelt behandling av personopplysninger, mens erklæringene er både kollektive og generelle, og må oppsøkes. Dette gjelder som et utgangspunkt også for § 19.¹¹⁵ Premisset for en slik vurdering må derfor være at vi godtar at pol.§ 19 er en form for standard i personvernlovgivningen for hva slags informasjon en registrert må antas å ha behov for, selv om § 19 verken kan begrunne bruken eller innholdet på egen hånd. En kan derfor ikke forvente full overenstemmelse med de krav § 19 oppstiller.

5.1.2 Informasjonsplikten vurdert opp mot innholdet i erklæringene

Både If og Storebrand gir omfattende informasjon i sine erklæringer, og brukerne får i ganske stor grad god informasjon om personopplysningsvernet. Det rettslige innholdet er tilnærmet likt i de to erklæringene, begge følger opp informasjons-, innsyns- og rettighetsreglene i loven, kun med noen små forskjeller. Etter § 19(1) bokstav a-e, jfr.§ 20(1), skal det som nevnt informeres om hvem som er behandlingsansvarlig, formålet, om opplysningene vil bli utlevert og til hvem, om det er frivillig å gi fra seg opplysningene, og annet som gjør den registrerte i stand til å "*bruke sine rettigheter*" etter personopplysningsloven.

Etter § 19(1) bokstav a skal både navn og adresse på den behandlingsansvarlige informeres om. If sier hvem som er behandlingsansvarlig, men nevner ikke adressen. Storebrand informerer verken om hvem som er behandlingsansvarlig for de ulike selskap i konsernet, og heller ikke adresse. Verken If eller Storebrand benytter derfor erklæringen til å gi den informasjonen bokstav a krever. Det følger av fal.§ 2-2 at det alltid skal inngås en skriftlig forsikringsavtale, og kundene vil da bli kjent med hvem som er behandlingsansvarlig. Den manglende informasjonen vil kun gjøre seg gjeldende for informasjon som samles inn før en slik avtale er inngått, og erklæringen vil ikke svekkes for mye overfor kundene til If og

¹¹⁵ Se imidlertid diskusjonen i kapittel 3.2.

Storebrand ved at dette ikke inkluderes. For brukerne av nettsiden som ikke er i et kunde-forhold, vil erklæringen ikke gi tilstrekkelig informasjon om hvem de skal kontakte.

Det skal etter § 19(1) bokstav b informeres om formålet med behandlingen, noe begge virksomheter gjør. Det vises til de konsesjonerte formål, og settes inn i en behandlings-sammenheng. Det er ikke fastsatt noe i forskriften om hvordan formålet skal angis ved gjennomføring av informasjonsplikten eller innsynsregelen,¹¹⁶ og for å oppfylle bokstav b er det nok tilstrekkelig å informere om de konsesjonerte formål så enkelt som det er gjort i erklæringene her. Videre bakgrunn for innsamling, og nærmere hva de brukes til, informeres også om, og kan nok sees på som overskuddsinformasjon som gjør den registrerte i stand til å ivareta sine rettigheter, jfr. bokstav e.

For å gi tilstrekkelig informasjon skal det informeres om opplysningene kan bli utlevert, og eventuell mottaker, jfr. § 19(1) bokstav c. Både If og Storebrand informerer om at person-opplysninger vil bli utlevert, og kommer til dels med eksempler på hvem som kan være mottaker. Hvem som er mottaker blir imidlertid ikke informert om på en tilstrekkelig måte av noen av dem, slik at informasjonsplikten ikke alene oppfylles av personvernerklæringene. If kunne også blant annet presisert deling med underleverandører i større grad, og forsikret brukerne om at deres databehandlere er underlagt samme formålsbegrensing som behandlingsansvarlig.

Etter § 19(1) bokstav d skal det opplyses om det er frivillig å gi fra seg opplysninger. Dette kan forstås som at det må informeres om det er lovhjemmel, samtykke eller annet som er behandlingsgrunnlaget. Å inngå en forsikringsavtale vil naturlig nok være frivillig, slik at den registrerte ikke vil trenge omfattende informasjon. Det kan særlig være et poeng å informere om de opplysninger som kan innhentes med grunnlag i lovgivning, og som da ikke er frivillig, slik at kundene blir kjent med at det vil være anledning til å innhente opplys-

¹¹⁶ Schartum(2012) note 53.

ninger også slik. Selve lovhjemmelen for innsamling bør da nevnes, for at den registrerte skal ha tilstrekkelig grunnlag for å vurdere gyldigheten av behandlingsgrunnlaget.¹¹⁷ Erklæringene gir noe informasjon om samtykke, men verken If eller Storebrand klarer å gi tilstrekkelig informasjon om behandlingsgrunnlaget for all deres innsamling av opplysninger. En kan nok si at en erklæring er egnet til å gi noe informasjon om frivillighet og hva en kan forvente å dele av opplysninger ved å inngå en avtale med de aktuelle selskaper, men at en virksomhet nok i de fleste tilfeller bør og må gi tilleggsinformasjon individuelt, for å oppfylle § 19(1) bokstav d. Erklæringene til If og Storebrand er på dette punktet mer til nytte for brukerne av nettsiden, enn kundene.

I pol.§ 19(1) bokstav e finner vi regelen om at det skal gis informasjon om annet som gjør den registrerte i stand til å "*bruke sine rettigheter*", noe som kan forklare at det gis informasjon om individuelle rettigheter i erklæringene. Bestemmelsen innebærer en plikt til å vurdere den registrertes behov for informasjon, slik at virksomheten pålegges å foreta en vurdering av personopplysningsvernet spesielt for sin virksomhet, og spesielt for de berørte brukere. For å oppfylle informasjonsplikten vil det likevel kunne være tilstrekkelig med generell informasjon om rettigheter, og informasjon om hvor en kan få videre individuell veiledning.¹¹⁸

Bestemmelsen kan også tolkes i lys av personverndirektivets art.10, som oppstiller et skille mellom "*essential information*" og "*further information*". Videre, utdypende informasjon skal bare gis i den utstrekning det er nødvendig, og sett i forhold til den konkrete behandlingssituasjonen.¹¹⁹ Også her ser vi at informasjonskravet påvirkes av form for behandling, og at virksomheter må vurdere erklæringene konkret opp mot sine kunder.

¹¹⁷ Johansen(2001) side 160.

¹¹⁸ Schartum(2012) note 92

¹¹⁹ WP 100

Det gis i § 19(1) bokstav e eksempler på informasjon som kan oppfylle en slik funksjon: informasjon om reglene om lagring, og om retten til å kreve innsyn og retting. Begge virksomheter gir informasjon både om disse forhold, men også om enkelte andre forhold som kan tolkes i lys av den registrertes rettigheter etter loven.

Av slik informasjon kan nevnes hvordan selskapene samler inn og lagrer opplysninger. Det informeres av begge at personopplysninger samles inn gjennom ulike kommunikasjonsmåter. Både gjennom telefonsamtaler, e-post og informasjonskapsler.

Omfanget av informasjon som gis om bruken av informasjonskapsler og analyseverktøy varierer. Ifs personvernerklæring gir omfattende informasjon, og brukere av nettsiden får god kunnskap om hva de elektroniske sporene brukes til. I tillegg gis informasjonen i eget dokument, slik at mottaker, brukeren av nettsiden, blir presisert. If kunne i tillegg gitt brukeren informasjon om hvilke verktøy som brukes, slik Storebrand gjør, men gjennom informasjon om hva som samles inn og hvordan de benyttes vil brukerne sitte igjen med tilstrekkelig informasjon til å ta et informert valg om nettaktivitet.

If gir god informasjon om lagring av telefonsamtaler. Lagring vil i seg selv være behandling av personopplysninger, og informasjon om dette må gis, med mindre det er åpenbart for den registrerte, jfr. § 19(1), jfr. (2). Det vil nok ikke være åpenbart at telefonsamtaler registreres, og heller ikke at e-postkommunikasjon lagres. Det vil derfor være avgjørende å informere, og erklæringene er en god kilde. Samtidig kan en ikke forvente at en person oppsøker en nettside i etterkant av en telefonsamtale for å lese om hvordan telefonsamtalen blir behandlet, og erklæringene kan sies ikke å være et tilstrekkelig verktøy i denne sammenheng.

For å gi mottakerne av erklæringene tilstrekkelig informasjon etter bokstav e, kunne begge selskaper inntatt informasjon om tilleggsvilkåret i konsesjonen om at:

*"Opplysninger knyttet til potensielle kunder (personer som har innhentet pristilbud) skal slettes så snart det blir klart at tilbudet ikke vil bli benyttet, og senest én måned etter akseptfristens utløp."*¹²⁰

Dette er informasjon som omhandler en gruppe som ikke er i et kundeforhold med selskapene, og da heller ikke har inngått en forsikringsavtale. Slik informasjon vil være særlig verdifull for å kunne bruke sine rettigheter, og en ser her en verdi av å ta med også dette i erklæringene, på vegne av brukerne av nettstedet.

5.1.3 Konklusjon

Storebrand oppfyller nok pol.§ 19(1) bokstav e på en noe mer utfyllende måte enn If; deres kunder blir i noe bedre stand til å "bruke sine rettigheter" etter loven gjennom erklæringen. Storebrand har gjennom den språklige presentasjonen en noe mer lett tilnærmelig erklæring, og brukerne vil nok få en bedre forståelse for den informasjonen de behøver gjennom denne. If er gjennomgående mindre informativ om hvorfor behandling av personopplysninger forekommer, og en får mindre generell kunnskap om personopplysningsvernet.

Likevel vil begge selskaper i stor grad oppfylle virksomhetens grunnleggende plikter etter pol.§ 19 så langt som mulig i en personvernerklæring, med noen unntak. If burde hatt med kontaktinformasjon, og Storebrand kunne med fordel inntatt en lenke til lovdata, og kanskje også til Datatilsynets nettsider. Dette er gode kilder for informasjon om personvern og bidrar å sikre ivaretagelse av personverninteresser. At If ikke informerer om at de har et personvernombud er en svakhet ved deres erklæring, dette kunne gitt deres kunder en mulighet til å benytte denne ressursen bedre.

¹²⁰ Datatilsynet(2011 b)

For de situasjoner der opplysninger innhentes fra andre, jfr.§ 20, møter nok erklæringene størst motgang. Det gis heller ikke tilstrekkelig informasjon om de forhold som kreves etter denne bestemmelsen av verken If eller Storebrand. For det første kan plikten til å informere i etterkant om at opplysninger er samlet inn om en, jfr.§ 20(1), klart ikke oppfylles gjennom en erklæring. Ved slik innsamling skal det for det andre informeres om hvilke opplysninger som er samlet inn, dette er det nok heller ikke særlig praktisk at forsikringsselskapene faktisk opplyser om i en erklæring.¹²¹ Se videre drøftelse av de særlige utfordringer ved innhenting av opplysninger fra andre i kapittel 5.2.2.

Undersøkelsen jeg har foretatt av erklæringene til If og Storebrand viser at selskapene alt i alt har gode personvernerklæringer, gjennom hensiktsmessig og informativ informasjon. Datatilsynet kom i sin rapport om personvernerklæringer til at If og Storebrand kom best ut av deres utvalg.¹²² På grunn av endringer i erklæringene siden da, ville både Storebrand og If kommet enda bedre ut i en tilsvarende undersøkelse nå. Forhold som tilgjengelighet er bedret, og begge virksomheter har et personvernombud for å nevne noe.

Personvernerklæringene til If og Storebrand bidrar til åpenhet om deres virksomhet, og informasjon gis utad både til brukere av nettstedet, allmenheten generelt, og til kunder av selskapene. Dette selv om erklæringene i seg selv ikke er tilstrekkelig sett opp mot informasjonsplikten personopplysningsloven oppstiller. Noe mer informasjon kunne vært inntatt, men erklæringene må sies å være av en informativ og grundig art.

¹²¹ Dette er likevel foreslått inntatt i en eventuell mal, se kapittel 4.4.1 og NOU 2009:1 side 124.

¹²² Datatilsynet(2011 a)

5.2 Generelle betraktninger og utfordringer ved personvernerklæringer

Ifølge Meld. St.11 (2012-2013) *Personvern – utsikter og utfordringer* er det igangsatt arbeid med å utforme en mal for personvernerklæringer.¹²³ Gjennom erfaringer gjort i undersøkelsen ovenfor vil jeg i denne sammenheng komme med noen generelle bemerkninger, og si noe om de utfordringer som følger med bruken av personvernerklæringer.

5.2.1 Informasjonen som gis

En personvernerklæring kan være et viktig dokument både for virksomheten og for brukerne av nettstedet. Utad kan den bekrefte at bedriften følger reglene for personvern, og innad potensielt være et styringsdokument for selve behandlingen av personopplysninger. Som vi så ovenfor i kapittel 5.1 er det ikke all informasjon som egner seg å gjengi i en erklæring. En personvernerklæring har først og fremst verdi som informasjon til allmennheten om hvordan virksomheten behandler personopplysninger. En erklæring vil sjelden være tilstrekkelig som informasjon til de som er registrert i virksomheten, jfr. vurderingen av pol.§19 gjort ovenfor, og ingen løfter kan nok bygges på dem. En offentlig tilgjengelig erklæring vil likevel gi muligheten for å vurdere behandlingsgrunnlaget, formål med behandlingen og om virksomheten følger norsk lovgivning, så fremt tilstrekkelig informasjon om dette gis. Datatilsynet uttaler at:

*"som et ledd i den demokratiske kontrollen er det viktig at borgeren gis informasjon, både for å ivareta egne rettigheter og for å kunne reagere på urettmessig eller for vid bruk av hjemler."*¹²⁴

Ved å gi informasjon om formål, og om konsesjon, vil både brukeren og allmennheten gis mulighet til å vurdere grunnlaget virksomheten er gitt for å behandle personopplysninger. Informasjon om behandlingsansvarlig vil gi kunnskap om hvem som kan holdes ansvarlig,

¹²³ Meld. St.11 (2012-2013) side 64

¹²⁴ Datatilsynet(2011 a)

det samme gjelder informasjon om utlevering og deling. Gjennom slik informasjon vil prinsippene om åpenhet og innsyn gis praktisk gjennomslag.

For virksomheter som offentliggjør endringer i sine erklæringer, noe som ofte vil si endret praksis innad, vil allmennheten få mulighet til å ytre kritikk mot behandlingen. Slik vi ser medier og tilsyn gjør når enkelte store virksomheter endrer sine erklæringer. Som et eksempel har vi Google Inc, som i 2012 gikk offensivt ut og informerte om at de hadde endret sin praksis, og med det sin "*privacy policy*". Blant mange gikk Artikkel 29-gruppen ut med kritikk av endringene, både i 2012¹²⁵ og nå i 2013.¹²⁶ Kritikken går både på deres faktiske personvernpraksis, men også på selve innholdet i erklæringen. For å bidra til åpenhet om at lovgivningen følges, kan det kanskje anbefales at virksomheten tar med informasjon om når erklæringen sist ble endret. Da vil en lettere kunne ta stilling til om det er foretatt tilpasninger til ny lovgivning.

5.2.2 Tidspunkt for informasjonen

På grunn av kravene til når informasjon må gis etter nåværende lovgivning, kan en diskutere om en personvernerklæring i det hele tatt kan oppfylle loven slik den er i dag. Plikten til å informere inntre på noe ulike tidspunkter avhengig av hvem opplysningene innhentes fra, sml. pol.§ 19 og § 20. Når opplysninger innhentes direkte fra brukeren av nettstedet, jfr.§ 19, vil plikten inntre før innsamling skjer, praktisk vil dette være i det behandling tar til å forekomme. Bestemmelsens ordlyd sier at den registrerte skal informeres "*først*", og av "*eget tiltak*", jfr.§ 19(1). Det vil si i det "*det samles inn*" personopplysninger. Virksomheter må derfor opplyse om dette før de har innhentet opplysninger. Når opplysninger innhentes fra andre enn brukeren vil den registrerte ha krav på informasjon "*så snart opplysningene er innhentet*", jfr. pol.§ 20(1) første setning, og da også om hvilke opplysninger som er innsamlet. Plikten til å gi informasjon utvides altså dersom opplysninger innhentes utenfra.

¹²⁵CNIL(2012)

¹²⁶WP Press Release(2013)

Der det samles inn opplysninger direkte gjennom nettstedet om brukere kan i enkelte tilfeller en lenke til erklæringen være tilstrekkelig til at de registrerte gis informasjon i tråd med § 19, forutsatt at innholdet også tilfredsstiller kravene.¹²⁷ For kunder av virksomhetene der det samles inn opplysninger på andre måter enn bare nettaktivitet, vil nok imidlertid en lenke på hjemmesiden være utilstrekkelig i og med at erklæringene må oppsøkes. Det kan ikke forventes at en kunde går inn på nettsiden og sjekker dersom selskapet etterspør en personopplysning for eksempel i en e-post eller over telefon. En personvernerklæring kan således være egnet til informasjon i forkant, sml.§ 19, men for å gi informasjon i etterkant, sml.§ 20, vil erklæringen være lite egnet, i og med at den registrerte selv må oppsøke den.

5.2.3 Ulike brukere krever ulik informasjon

I NOU 2009:1 er ett av forslagene til normplakat om personvern at det i personvernerklæringer skal informeres om hvilke personopplysninger som samles inn.¹²⁸ Det vil ikke alltid være helt praktisk. For det første er en erklæring en kollektiv tekst, og hva som samles inn vil ofte være ulikt fra kunde til kunde. For det andre er erklæringene ofte ikke engang tilpasset ulik virksomhet som drives, slik vi ser hos konsernet Storebrand som driver både forsikringsvirksomhet og finansvirksomhet, med mer. Et kompromiss kan være at en gir generell informasjon om hvilke institusjoner opplysninger kan komme til å bli samlet inn fra, slik vi ser gjøres til dels hos If og i noe mindre grad av Storebrand.

Datatilsynets og Ifs bruk av to erklæringer gjenspeiler noen av utfordringene med personvern over internett. Innholdet bør tilpasses mottakeren, men mottakeren kan være mange. Erklæringen kan, og bør, tilpasses til om mottakeren kun er besøkende av nettstedet, eller også er kunde av virksomheten, slik Datatilsynet og If gjør. Videre også etter ulike kundetyper, noe Storebrand kunne ha gjort.

¹²⁷ Datatilsynet(2005)

¹²⁸ NOU 2009:1 side 124.

Det er viktig at en virksomhet foretar en konkret vurdering av hvilke utfordringer som særlig gjør seg gjeldende for deres virksomhet innen personvern. Dette innebærer å utrede hvilke rettigheter deres brukere har, hvilke krav brukerne kan stille til virksomheten og hvilke plikter som påligger virksomheten. Dette følger også av pol.§ 19(1) bokstav e. En som kun besøker et nettsted for å finne informasjon om for eksempel et tilbud, eller for å foreta et nettkjøp, vil ha behov for helt annen informasjon enn en som har et langvarig kundeforhold til virksomheten. En kan si at har en behov for kun litt informasjon, skal en slippe å måtte lese gjennom et langt dokument med irrelevant tekst før en finner det en leter etter.

Å tilpasse innholdet til sine egne brukere vil også bety å se an forhold som alder og kunnskapsnivå. En nettside som benyttes av barn vil kunne stille helt spesielle krav til informasjonen som gis. Dette er også påpekt i Meld. St.11 (2012-2013),¹²⁹ og det ble i 2011 inntatt en bestemmelse om særlig krav ovenfor barn i forbindelse med behandlingen i pol.§ 11(3). At leseren er en alminnelig person, som regel uten juridisk utdanning, stiller også krav til innhold og språk. En kunde av en virksomhet vil ofte være det vi i juridisk forstand forstår som en forbruker, noe en bruker av en nettside også kan anses som i enkelte tilfeller, der den ene sitter med mer kunnskap og oversikt over det aktuelle området enn den andre. Forholdet mellom leser av en erklæring og avgiveren vil derfor til en viss grad være sammenlignbart med forholdet mellom en forbruker og en selger. Dette bør vurderes av den enkelte virksomhet og få utslag i språket.

En annen utfordring angår det at erklæringene er kollektive, lik informasjon gis til alle. I forarbeidene til § 19 anføres det at varslingen i utgangspunktet skal være individuell, med mindre dette ikke er mulig. Først da hevdes det at kollektiv varsling kan anvendes.¹³⁰ Som nevnt er det liten kontakt mellom brukeren av en nettside og den som driver nettsiden, og bruken av personvernerklæringer må nok aksepteres som en fornuftig løsning for å gi til-

¹²⁹ Meld. St.11 (2012-2013) side 65.

¹³⁰ Ot.prp.nr.92 (1998-1999) side 120.

strekkelig informasjon i enkelte tilfeller. Forutsetningen er liten kontakt, at den aktuelle informasjon er egnet til å gis på denne måten, og at det ikke er andre måter som er bedre egnet. Dette må vurderes konkret av virksomheten. I pol.§ 20(2) oppstilles en avveining om at varsel ikke er påkrevd dersom det er "*umulig eller uforholdsmessig vanskelig*". Selv om det ikke er umulig eller uforholdsmessig vanskelig å gi individuell informasjon kan det nok være et poeng å se disse to vurderinger i sammenheng.

Mye av innhenting av personopplysninger skjer gjennom innsending av nettskjema, gjennom e-post og gjennom bevegelse på nettstedet. Å sende en avtale i posten før behandling av personopplysninger vil ikke alltid være praktisk mulig. Slik vil alternativet personvernerklæring påvirke vurderingen av hva som er "*umulig eller uforholdsmessig*" også den motsatte veien; dersom personvernerklæringer aksepteres som et godt alternativ for informasjon vil det vanskelig sies å være uforholdsmessig å ha dette. Nettopp her kan en se den selvstendige verdien av personvernerklæringer.

5.2.4 Er loven tilpasset nyere teknologi?

Internett kan ikke lenger sies å være et nytt medium, men teknologien som benyttes utvikles stadig og skaper utfordringer på flere områder. Det kan derfor være interessant å se på om loven er tilpasset denne nye teknologien, knyttet opp til den informasjonen som gis i erklæringer. Dersom en virksomhet ønsker å tilpasse innholdet i erklæringen til lovens regler om informasjonsplikt, jfr. pol.§ 19 og § 20, er det et uklart spørsmål som oppstår. For tilfeller der det samles inn identifiserbare opplysninger gjennom analyseverktøy, altså personopplysninger, jfr. pol.§ 2 nr.1, vil det kunne reises spørsmål om innhenting av opplysninger på denne måten faller innunder opplysninger som innhentes "*fra den registrerte selv*", eller fra andre, sml.§ 19 og § 20. Gjennom bruk av webanalyseverktøy får virksomheter informasjon om brukeren, gjennom brukerens egen aktivitet på internett, noe som tilsier at dette må være innhenting fra den registrerte selv. Med dette er behandlingen unnatt informasjonsplikt om *hvilke* opplysninger som innhentes, jfr.§ 19, sml.§ 20. Etter lovens ordlyd vil ikke virksomheten, den behandlingsansvarlige, ha noen plikt til å opplyse hvilken informasjon som samles inn, selv om brukeren ikke selv bevisst gir fra seg person-

opplysninger. De behøver da kun å opplyse om at det samles inn, mens det for å få vite hvordan og hva slags opplysninger som er innsamlet må kreves innsyn om etter pol.§ 18.

Bak skillet mellom § 19 og § 20 ligger at en vet hvilke opplysninger en gir fra seg når det er en selv som gir de ut. En bruker av en nettside vil ikke nødvendigvis ha kjennskap til at han gir fra seg opplysninger i en slik situasjon, og hensynet bak manglende plikt til å gi informasjon gjør seg ikke gjeldende på samme måte her. Dette er en utfordring i lovens ordlyd. For elektroniske spor er dette søkt løst gjennom forslag til ny ekomlov, men det er fortsatt viktig å skille mellom hva som er en personopplysning og hva som kun er et elektronisk spor innhentet fra en person. Forslaget til ny personvernforordning søker også å dekke opp bedre de nye utfordringer som kommer med økt internettbruk, blant annet gjennom forslaget om at alle skal få god og tydelig informasjon i en personvernerklæring publisert på nettsiden, jfr. foreslått art.11.¹³¹

5.2.5 Lovfesting

Det er foreløpig liten veiledning å få fra offentlig hold om personvernerklæringer, og de fleste anbefalinger som kommer er "bør"-anbefalinger, enten i form av bransjenormer eller som veiledning fra Datatilsynet. Dette kan nok gjøre det utfordrende for de virksomheter som ønsker å vise åpenhet og gi informasjon til sine kunder.

En kan stille spørsmål om en kan sikre et tilstrekkelig brukervern uten en lovfesting av bruken av personvernerklæringer. Et konkret spørsmål oppstår dersom bruken av erklæringer lovfestes; hvordan skal en oppstille klare nok kriterier for å avgjøre om regelen er oppfylt? Det kan ikke være nok å ha en tekst publisert med tittelen "*personvernerklæring*", innholdet må også oppfylle et bestemt krav. Noen momenter vil det være enkelt å avgjøre om er på plass, men en kan tenke seg at en vurdering som må tas i hvert enkelt tilfelle er om "*erklæringen er tilstrekkelig informativ*". Dette er ikke en enkel oppgave.

¹³¹ Forordning 2012/0011 (KOM)

Det må også stilles spørsmål om det skal lovfestes at absolutt alle virksomheter som behandler personopplysninger må ha en slik erklæring, eller om det bare skal gjelde for eksempel virksomheter av en viss størrelse. I tillegg må en nok ta stilling til hva slags behandling som skal utløse et slikt krav; kun ved omfattende behandling som en del av virksomheten, eller skal det også gjelde for virksomheter som kun behandler opplysninger som en sideeffekt av å ha en nettside?

Om ikke lovhjemmel fastsettes kan en tenke seg at pålegg om erklæring kan inntas i konsesjonen. Om dette er en god løsning vil være åpent for vurdering. En utarbeidelse av en normplakat eller en mal er kanskje en god start, og en vil da kunne få verdifull informasjon om hvordan etterlevelse vil forekomme, før en eventuell lovfesting. Likevel ser vi utfordringer også med en mal, det skal vanskelig gjøres å lage én mal som passer alle former for virksomhet. Informasjonsreglene vi har i dag oppstiller krav om individuell informasjon,¹³² noe en erklæring klart ikke kan gi. Det vil være vanskelig å oppfylle alle informasjonskrav i en kollektiv erklæring. Heller ikke alle krav i § 19 viser seg egnet for å tas med i en erklæring, noe som gjør at en personverklæring først og fremst blir en tilleggskanal for informasjon. Formen informasjonen gis på i en erklæring er derfor ikke helt lett å kombinere med informasjonskravene i loven, og både eventuell lovfesting eller en mal utarbeidet av Data-tilsynet må ta hensyn til dette.

5.2.6 Erklæringene må leses

I en drøftelse av personvernerklærings verdi er en nødt til å kommentere hvor tilgjengelig informasjonen faktisk er gjennom antallet lesere. En europeisk undersøkelse fra 2011 presentert av EU-kommisjonen viser at 6 av 10 (58 %) "*usually*", vanligvis, leser slike erklæringer.¹³³ Dette er relativt mange, men undersøkelsen kan nok ikke forstås slik at 6 av 10

¹³² Ot.prp.nr.92 (1998-1999) side 120.

¹³³ European Commission(2012)

"alltid" leser slike, gitt ordlyden i resultatet. Jeg vil være litt forsiktig med å trekke slutninger om hvor mange som leser slike erklæringer på et generelt grunnlag. Det er nok grunn til å anta at det først og fremst er de som søker slik informasjon som faktisk finner frem til erklæringene. Verdien av informasjonen som gis reduseres dersom ingen eller veldig få får med seg informasjonen. Imidlertid kan en ikke tvinge folk til å lese om forhold vedrørende deres eget personvern.

Mange vil nok kunne tenke at hos store virksomheter så er det "*noen*" som har lest og vurdert forhold vedrørende personvernet "*for én*". Dersom store selskaper med mange brukere endrer personvernerklæringen sin får det ofte oppslag i aviser, og en kan kanskje si at media passer på, til en viss grad. I en undersøkelse foretatt i 2004 av Teknologirådet om lekfolks holdninger til personvern uttales det at det var få av deltakerne som leste personvernerklæringer. Det ble sagt at slike dokumenter er "*alt for lang[e] og tidkrevende å lese*" og ble oppfattet som "*ganske unødvendig*" av deltakerne i undersøkelsen. Likevel ble det blant de unge deltakerne etterlyst mer informasjon, særlig om elektroniske spor som cookies, og det fremsettes ønske om informasjon om hvordan teknologien fungerer og hvordan man i større grad kan beskytte seg selv. For eksempel gjennom informasjon om hvordan man kan slette cookies.¹³⁴

Resultatene må sees i lys av å være innhentet for 9 år siden, men kan tyde på at utviklingen med mer informasjon om bruken av informasjonskapsler og webanalyseverktøy har vært ønsket. Personvern er noe som får økende oppmerksomhet i samfunnet, og med tiltagende krav til at virksomheter er nødt til å ha en erklæring tilgjengelig vil en kunne anta at antall lesere øker. I en rapport utført av Sintef i 2009 kommer det frem at 67 % av nettbrukere er bekymret for konsekvensen av å dele personlige opplysninger på internett.¹³⁵ Undersøkelsen er knyttet til bruken av sosiale medier, og gjerne utenlandske nettsider, og er derfor ikke direkte overførbar til interessen for personvern innen området som er undersøkt i den-

¹³⁴ Teknologirådet(2004)

¹³⁵ Brandtzæg(2009)

ne oppgaven. Likevel sier det noe om en bevissthet hos folk om personvern ved bruk av internett.

Rettsområdet kan være utfordrende å sette seg inn i, og enkel innføring i dette vil være givende. At informasjonen er lett tilgjengelig gjennom språket, og satt inn i en rettslig pedagogisk sammenheng, må være et mål. For mye informasjon vil gjøre at erklæringene ikke leses, og vil virke mot sin hensikt. Det er viktig å ikke stille for store krav til omfanget av informasjon som gis. Erklæringen kan ha potensiale til å gi sentral informasjon på ett sted, dette må utnyttes ved å ikke gjøre informasjonen utilgjengelig nettopp for dem som er ønsket mottaker. En personvernerklæring er et godt og hensiktsmessig redskap for å bidra til kunnskap og forståelse, og virksomheter bør ha et bevisst forhold til utarbeidelsen av en god erklæring, tilpasset sin aktivitet.

6 Kilder

6.1 Lover

1989	Lov om forsikringsavtaler (forsikringsavtaleloven (fal.)) av 16. juni 1989 nr. 69
1992	Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS-loven) av 27.november 1992 nr. 109
2000	Lov om behandling av personopplysninger (personopplysningsloven (pol.)) av 14. april 2000 nr. 31
2003	Lov om elektronisk kommunikasjon (ekomloven) av 4. juli 2003 nr. 83
2005	Lov om forsikringsselskaper, pensjonsforetak og deres virksomhet mv. (forsikringsvirksomhetsloven (fvl.)) av 10. juni 2005 nr. 44
2009	Lov om kontroll med markedsføring og avtalevilkår mv. (markedsføringsloven) av 9.januar 2009 nr. 2

6.2 Forskrifter

2000	Forskrift om behandling av personopplysninger (personopplysningsforskriften (pof.)) av 15. desember 2000 nr. 1265
------	---

6.3 Forarbeider

NOU 1997: 19

Et bedre personvern

Ot.prp.nr.92 (1998-1999)

Om lov om behandling av personopplysninger

NOU 2009: 1

Individ og integritet. Personvern i det digitale samfunnet

Meld. St. 11 (2012-2013)

Personvern – utsikter og utfordringer

Prop. 69 L (2012-2013)

Endringer i ekomloven

6.4 Rettsavgjørelser

Rt-2005-451

Forsikringsvirksomhetsloven § 12-2 første ledd ble av kjæremålsutvalget forstått slik at den innenfor rammen av generalagentens kompetanse til å forplikte selskapet ga den norske filialen partsevne med generalagenten som stedfortreder.

6.5 Direktiver

Direktiv 95/46/EF

Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personverndirektivet)

Direktiv 2009/136/EF

Europaparlaments- og rådsdirektiv 2009/136/EF av 25. november 2009 som endrer direktiv 2002/22/EF om universelle tjenester og brukerrettigheter, direktiv

2002/58/EF om kommunikasjonsvern og forordning (EF) nr. 2006/2004 om samarbeid om forbrukerbeskyttelse (cookie-direktivet)

Forordning 2012/0011 (KOM)

Forslag til europaparlaments- og rådsforordning om vern av personer med hensyn til behandling av persondata og om fri utveksling av slike data (personvernforordningen)

6.6 Avgjørelser av Personvernemnda

PVN-2004-08

Klage på konsesjonsvilkår om behandling av personopplysninger i forsikringsbransjen

PVN-2007-01

Arvelighetsregisteret

PVN-2010-06

Forsikringsselskaps bruk av kredittopplysninger

PVN-2011-06

ConocoPhillips

6.7 Uttalelser fra Artikkel 29-gruppen

WP 43

Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union. URL:

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp43en.pdf> [sitert 10.3.2013]

WP 100

Opinion 10/2004 on More harmonised information provisions. URL:

	http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf [sitert 10.3.2013]
WP 153	Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules. URL: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm [sitert 10.3.2013]
WP 194	Opinion 04/2012 on Cookie Consent Exemption URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf [sitert 10.3.2013]
WP 202	Opinion 02/2013 on apps on smart devices. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf [sitert 19.03.2013]
WP Press release	Google's privacy policy: European data protection authorities are coordinating their enforcement actions. Brussel 2013. URL: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130227_pr_google_privacy_policy_en.pdf [sitert 06.04.2013]

6.8 Bøker

Blixrud, Katrine Berg og Christine Ask Ottesen. Personvern i finanssektoren. Gyldendal forlag, Oslo, 2010.

Johansen, Michal Wiik, Knut-Brede Kaspersen og Åste Marie Bergseng Skullerud. Personopplysningsloven, Kommentarutgave. Universitetsforlaget, Oslo, 2001.

Schartum, Dag Wiese og Lee A. Bygrave. Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger. 2. Utgave. Fagbokforlaget, Oslo, 2011.

6.9 Nettdokumenter

Brandtzæg, Petter Bae og Marika Hanne Lüders. SINTEF rapport Privat 2.0: Person- og forbrukervern i den nye medievirkeligheten. 2009. URL:

<http://www.sintef.no/upload/Konsern/Media/Person%20og%20forbrukervern.pdf> [sitert 9.4.2013]

CNIL. Brev til Google Inc. på vegne av Artikkel 29-gruppen. Paris 2012. URL:

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120227_letter_cnil_google_privacy_policy_en.pdf [sitert 14.3.2013]

Datatilsynet. Konesjon bank og finansinstitusjoner. Oslo 2005. URL:

http://datatilsynet.no/Global/05_regelverk/Konesjoner/bankkonesjon.pdf [sitert 6.4.2013]

Datatilsynet. Fortell meg hva dere gjør! Oslo 27.juni 2011 a. URL:

http://www.datatilsynet.no/Global/04_analyser_utredninger/2011/30062011_Nettkontroller_2010_-_analyse.pdf [sitert 6.4.2013]

Datatilsynet. Konesesjon forsikring. Oslo 2011 b. URL:

http://datatilsynet.no/Global/05_regelverk/Konesesjoner/Konesesjon_forsikring.pdf [sitert 6.4.2013]

Datatilsynet. Overføring til utlandet. Oslo 2011 c. URL:

<http://www.datatilsynet.no/Sektor/Overfoering/> [sitert 6.4.2013]

Datatilsynet. Overføring til utlandet. Oslo 2011 d. URL:

<http://www.datatilsynet.no/Sektor/Overfoering/#Standardkontrakt> [sitert 8.4.2013]

Datatilsynet. Safe Harbor-prinsippene. Oslo 2011 e. URL:

<http://datatilsynet.no/Sektor/Overfoering/Safe-Harbor-prinsippene/> [sitert 20.4.2013]

Datatilsynet. Bør ha personvernerklæring på nett. Oslo 2012 a. URL:

<http://datatilsynet.no/Nyheter/Nyheter-2011/Bor-ha-personvernerklaring-pa-nett/> [sitert 6.4.2013]

Datatilsynet. Datatilsynets personvernerklæring. Oslo 2012 b. URL:

<http://datatilsynet.no/Om-Datatilsynet/Datatilsynets-nettsider/Personvernpolicy/> [sitert 6.4.2013]

Datatilsynet. Personvernerklæring for datatilsynet.no. Oslo 2012 c. URL:

<http://datatilsynet.no/Om-Datatilsynet/Datatilsynets-nettsider/> [sitert 6.4.2013]

Datatilsynet. Bruk av webanalyseverktøy. Oslo 2012 d. URL:

<http://datatilsynet.no/Teknologi/Webanalyse/> [sitert 6.4.2013]

Datatilsynet. Virksomheter med ombud. Oslo 2013 a. URL:

<http://datatilsynet.no/Personvernombud/Virksomheter-med-ombud/> [sitert 6.4.2013]

Datatilsynet. Mener at bruk av Google Analytics er lovstridig. Oslo 2013 b. URL:
<http://datatilsynet.no/Nyheter/2012/Mener-at-bruk-av-Google-Analytics-er-lovstridig-/>
[sitert 8.4.2013]

Datatilsynet. Endelig kontrollrapport Skattedirektoratet. Oslo 2013 c. URL:
http://datatilsynet.no/Global/05_tilsynsrapporter/2011/11-00906-9%20Endelig%20kontrollrapport_Skattedirektoratet.pdf [sitert 7.4.2013]

Datatilsynet. 7 steg til innebygd personvern. Oslo 2013 d. URL:
<http://datatilsynet.no/Teknologi/Innebygd-personvern/> [sitert 14.3.2013]

Electronic Frontier Foundation. Best practices for online providers. 2008. URL:
<https://www.eff.org/wp/osp> [sitert 6.4.2013]

European Commission. How will the EU's data protection reform simplify the existing rules? Brussel 2012. URL: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/6_en.pdf [sitert 6.4.2013]

If. Behandling av personopplysninger. Oslo 2013 a. URL:
<http://www.if.no/web/no/omnettstedet/pages/behandlingavpersonopplysninger.aspx> [sitert 13.2.13]

If. Bruk av cookies og elektroniske spor. Oslo 2013 b. URL:
<http://www.if.no/web/no/omnettstedet/pages/cookies.aspx> [sitert 3.4.13]

If. Om oss. Oslo 2013 c. URL: <http://www.if.no/web/no/om/fakta/styre/pages/default.aspx>
[sitert 7.4.2013]

International Conference of Data Protection and Privacy Commissioners. The Madrid Resolution on international standards on the protection of personal data and privacy. Madrid 2009. URL: <http://www.gov.im/lib/docs/odps/madridresolutionnov09.pdf> [sitert 20.2.2013]

International Conference of Data Protection and Privacy Commissioners. Resolution on Privacy by Design. Jerusalem, Israel 2010. URL: http://datatilsynet.no/Global/english/ResolutiononPrivacybyDesign_2010.pdf [sitert 8.4.2013]

Storebrand. Personopplysninger. Oslo 2013 a. URL: http://www.storebrand.no/site/stb.nsf/Pages/samfunnsansvar_personopplysninger.html [sitert 13.2.13]

Storebrand. Fakta om Storebrand. Oslo 2013 b. URL: <http://www.storebrand.no/site/stb.nsf/Pages/hovedsidefaktaomstorebrand.html> [sitert 16.4.2013]

Reiersen, Hedvig Bugge og Beate Sjøfjell. NUF-kaoset i norsk rett – et bidrag til oppklaring. Tidsskrift for rettsvitenskap 2010 s. 423-462. (Sitert fra lovdata)

Schartum, Dag Wiese. Kommentar til personopplysningsloven. Norsk lovkommentar nettversjon, sist revidert 18.10.2012. [sitert 8.4.2013]

Teknologirådet. Holdninger til personvern, Rapport fra fokusgrupper om elektroniske spor og personvern. Oslo 2004. URL: http://teknologiradet.no/Rapport_fokusgrupper_9-5lz.pdf.file [sitert 6.4.2013]

Webanalytiker. Verktøy for webanalyse og webstatistikk. 2013. URL: http://www.webanalytiker.net/fordeler_og_ulemper_oversikt_webanalyseverktoy_google_omniture_webtrends.html [sitert 6.4.2013]

6.10 Nettsider til de mest brukte kilder

Artikkel 29-gruppen http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

Datatilsynet www.datatilsynet.no

Electronic Frontier Foundation <https://www EFF.org/>

Lovkommentar nettversjon www.reettsdata.no

If Skadeforsikring NUF www.if.no

Rettskilder www.lovdato.no

Storebrand AS www.storebrand.no

7 Vedlegg

Vedlegg 1 Behandling av personopplysninger – if.no¹³⁶

Vedlegg 2 Slik behandler vi personopplysninger – storebrand.no¹³⁷

Vedlegg 3 Cookies – if.no¹³⁸

¹³⁶ If (2013 a)

¹³⁷ Storebrand (2013)

¹³⁸ If (2013 b)



Startside No Privat Bedrift Om If

Om nettstedet

Om nettstedet

Vedlegg 1

Behandling av personopplysninger

Personopplysninger er opplysninger og vurderinger som kan knyttes til en enkeltperson, for eksempel navn, adresse, telefonnummer og e-postadresse.

Behandling av personopplysninger vil i følge personopplysningsloven si enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Behandlingsansvarlig

If Skadeforsikring NUF (org.nr. 981 290 666) er behandlingsansvarlig, og skal behandle personopplysninger innen rammen av gjeldende lov og forskrift, samt Datatilsynets konsesjon til å behandle slike opplysninger. If har konsesjon til å behandle personopplysninger for kundeadministrasjon, fakturering og gjennomføring av forsikringsavtaler i tråd med reglene i forsikringsvirksomhetsloven og forsikringsavtaleloven.

Innhenting av personopplysninger

If innhenter personopplysninger fra kunden selv, representanter for kunden, kredittinformasjonsregistre og offentlige registre.

Ifs behandling av personopplysninger

De personopplysninger som innhentes er nødvendige for at selskapet skal kunne administrere forsikringer, oppfylle selskapets avtaleforpliktelser og forevrig kundes ønsker. Opplysningene vil kunne bli benyttet for å vurdere og fatte beslutninger om forsikrings innhold og vilkårsutforming, samt i markedsanalyser og markedsføring.

Personopplysningene kan for de nevnte formål også utleveres til selskap/organisasjoner If Skadeforsikring samarbeider med, så vel innenfor som utenfor EØS- og EU-området. Dersom If Skadeforsikring har opplysningsplikt overfor offentlig myndighet, vil opplysninger bli overlevert i henhold til myndighetenes krav.

Opplysningene vil også kunne bli benyttet til å gi kunden informasjon om selskapets/samarbidsorganisasjonens tjenester forøvrig.

Opplysningene utleveres også til fellesregistrene for forsikringsbransjen ROFF og FOSS. Formålet med ROFF er å bedre og sikre en ensartet risikobedømmelse ved premiefastsettelse, samt til kontroll med sikte på å unngå spekulasjon. FOSS har til formål å forhindre forsikringssvindel.

Helseopplysninger

Dersom det i forbindelse med forsikringsforholdet er behov for innhenting av helseopplysninger, ber If alltid om samtykke fra den opplysningen gjelder. Helseopplysninger behandles og lagres i egne systemer med streng tilgangsbegrensning, og behandles bare av en svært begrenset krets ansatte som har tjenestlig behov.

Reservasjon

I henhold til markedsføringsloven § 12 kan du reservere deg mot å motta markedsføring fra If og våre samarbeidspartnere.

Innsyn og retting

I henhold til personopplysningslovens § 18 har man krav på innsyn i de opplysninger som er registrert. Innsyn kan fås ved å sende en skriftlig henvendelse til If. Henvendelsen må inneholde polisenummer eller personnummer, samt være underskrevet av den registrerte.

Dersom de registrerte opplysninger ikke er riktige eller de er ufullstendige kan du kreve disse rettet i henhold til personopplysningslovens § 27.

Opptak og lagring av kundekommunikasjon

Som et ledd i kontinuerlig forbedring, kvalitetssikring og effektiv kundebehandling tas det opptak av telefonsamtaler til våre kunde- og skadesentre. Når det tas opptak, blir det avspilt en automatisk talebeskjed som informerer om dette før samtalen starter. Disse lydopptakene og annen dokumentasjon av kommunikasjonen med

kunder, f. eks. chat og e-post, oppbevares i tre år. Telefonsamtaler kan søkes opp basert på telefonnummer, dato/tid og hvilken medarbeider som var involvert i kundekontakten. Tilgang til avspilling av telefonsamtaler er strengt begrenset til de som har et tjenstlig behov og all tilgang til samtaler blir loggført med en kort begrunnelse hver gang avspilling foretas. Kopi av andre kommunikasjonsformer (chat, e-post o.l.) kan gjenfinnes etter kundidentitet, tidspunkt, medarbeider eller annen egnet informasjon.

Oppbevaring og sletting

I henhold til personopplysningslovens § 28 skal opplysninger som ikke lenger er nødvendig ut fra det formål de er lagret for slettes.

If lagrer personopplysninger om kunder i henhold til den enhver tid gjeldende lovgivning.

Databilsynet (nytt vindu)

Personopplysningsforskriften (nytt vindu)

Personopplysningsloven (nytt vindu)

© If Skadeforsikring NUF [Behandling av personopplysninger](#) [Cookies](#) [Sidekart](#) [Tilpass](#)

[If skadeforsikring SE](#) [If Skadeforsikring DK](#) [If Vahinkovakuutusyhtiö FI](#)

Vedlegg 2

Personopplysninger

Personvernombud

Storebrand tar behandling av personopplysninger på alvor. Vi har opprettet et eget personvernombud som har i oppgave å drive opplæring internt i virksomheten om behandling av personopplysninger, samt å påse at denne behandlingen foregår i henhold til gjeldende lover og regler.

Personvernombudet er også en ressursperson for deg som kunde. Om du lurer på noe rundt Storebrands behandling av personopplysninger, eller du har innspill til oss vedrørende dette temaet, kan du kontakte vårt kunde- og personvernombud på e-post kundeombudet@storebrand.no

Innhenting av personopplysninger

For å kunne innfri våre forpliktelser overfor deg som kunde trenger Storebrand informasjon om deg. Datatilsynet har gitt Storebrand konsesjon for å behandle personopplysninger til nærmere angitte formål:

- Kundeadministrasjon, fakturering og gjennomføring av forsikringstjenester og bank- og finansieringstjenester.
- Markedsføring og kundecoppfølging.
- Risikoklassifisering av kunder og kredittporteføljer.
- Forebygging og avdekking av straffbare handlinger.

Storebrand innhenter som regel opplysningene direkte fra deg som kunde. Noen ganger innhenter vi opplysninger fra andre, for eksempel offentlige eller private institusjoner. Du vil bli informert dersom vi innhenter opplysninger om deg, med mindre innsamlingen er lovbestemt, varslings er umulig eller uforholdsmessig vanskelig eller det er på det rene at du allerede kjenner til de opplysningene varselet skal inneholde.

Storebrand benytter ved tilfeller e-post som kommunikasjonskanal mot våre kunder. Vi vil understreke at vi i vår e-postkommunikasjon aldri vil be om sensitive, fortrolige eller konfidensielle opplysninger. Vi kan ikke garantere at meldinger som sendes med e-post via det alminnelige nett ikke blir kjent for andre. Vi anbefaler derfor ikke at sensitive opplysninger sendes med alminnelig e-post. Trygg oversendelse av sensitive opplysninger til oss kan gjøres gjennom dine personlige sider.

Konsernsamtykke

For at vi skal kunne gi deg best mulig kundeservice, samt informasjon og tilbud om de produkter og tjenester vi tilbyr kan du gi det vi kaller konsernsamtykke. Dette kan du gjøre på dine personlige sider.

Konsernsamtykke innebærer at opplysningene om deg blir tilgjengelig for alle selskapene i Storebrand konsernet. Med tilgang til flere av opplysningene vi har registrert om deg sørger vi for at rådgivning og tilbud er bedre tilpasset dine behov. Konsernsamtykket gjelder ikke bruk av sensitive opplysninger, som for eksempel helsesituasjon eller uforhet.

Hva bruker Storebrand opplysningene til?

Storebrand er forpliktet til å behandle opplysningene fra sine kunder på en forsiktig måte. Det er personopplysningsloven med forskrift og konsesjonen fra Datatilsynet som har regler for hvordan denne behandlingen skal foregå.

Opplysningene vi har registrert om deg brukes i all hovedsak til å følge opp deg som kunde, blant annet å informere deg om de produktene du har hos oss.

Spesielt om bruk til markedsføring

Såkalte nøytrale kundeopplysninger (navn, adresse, fødselsår, kjønn og kontaktopplysninger) og opplysninger om hvilke produkter du allerede har inngått avtale om kan brukes som grunnlag for informasjon og markedsføring av eksisterende og nye tjenester og produkter.

Bruk av opplysninger som ikke er nøytrale, for eksempel transaksjonsopplysninger og andre dybdeopplysninger om kundeforholdet og bruk av tjenestene kan bare brukes i markedsføringsøyemed dersom det foreligger et frivillig, informert og uttrykkelig samtykke fra deg som kunde. Slikt samtykke kan du gi på dine personlige sider.

Slik videreformidler vi personopplysninger

Storebrand har taushetsplikt om kundeopplysninger. Likevel kan det være aktuelt å videreformidle opplysningene dersom du som kunde har samtykket til dette eller i tilfeller Storebrand er forpliktet i henhold til lov å overlevere slike opplysninger.

Internt i Storebrandkonsernets selskaper har vi et felles kunderegister som er tilgjengelig for alle konsernselskapene. Formålet med dette konsernkunderegisteret er å oppnå størst mulig samordning av tilbudet av tjenester og rådgivning fra de forskjellige selskapene i konsernet. Kunderegisteret vil kunne inneholde navn, fødselsnummer, adresse og kontaktopplysninger, opplysninger om hvilket konsernselskap du er kunde i og hvilke tjenester og produkter du har avtale om. Utlevering og registrering av andre personopplysninger i kunderegisteret krever samtykke fra deg.

I noen tilfeller krever loven at vi utleverer opplysninger til andre, blant annet offentlige myndigheter. I slike tilfeller vil opplysninger om deg kunne bli utlevert uten ditt samtykke.

Vi har også noen underleverandører som vil kunne ha behov for opplysninger om deg. Når vi deler opplysninger med våre underleverandører regnes ikke dette som utlevering av opplysninger, og denne delingen av opplysninger reguleres av databehandleravtaler. Våre underleverandører behandler personopplysninger på vegne av Storebrand, og vil kun bruke opplysningene til de formål de er innhentet.

Lagring av opplysningene

Opplysningene vi har om deg lagres blant annet i vårt felles kunderegister og i ulike saksbehandlingssystemer. Dette gjøres for å kunne gi deg god informasjon, for å ha en historie på ditt kundeforhold hos oss og for å kunne gi deg svar på eventuelle spørsmål du måtte ha i forbindelse med ditt kundeforhold hos oss.

Opplysningene lagres så lenge det er nødvendig for å oppfylle formålet med behandlingen. Det vil i praksis si så lenge avtaleforholdet eksisterer. Dersom avtalen sies opp, vil Storebrand på grunn av muligheten for fremtidige erstatningskrav som kan tilbakeføres til avtaleforholdet, lagre opplysningene frem til foreldelsesfristen for de aktuelle produktene er utløpt.

Dine rettigheter

Innsyn

Du har rett til å få informasjon om de opplysningene om deg vi behandler og hvordan vi behandler dem. En god del av den informasjonen vi har om deg som kunde ligger på [dine>http://www.storebrand.no/site/stb.nsf/Pages/forsideperson.html](http://www.storebrand.no/site/stb.nsf/Pages/forsideperson.html).

Retting/sletting

Det er viktig at opplysningene vi har om deg er riktige og at de er nødvendige. Du kan kreve å få rettet opp opplysninger om deg dersom opplysningene er mangelfulle eller unødvendige.

Storebrand vil slette de registrerte opplysningene når vi ikke lenger har bruk for dem for å oppfylle det formålet som vi innhentet opplysningene for. Dette innebærer at så lenge avtaleforholdet eksisterer vil opplysningene være registrert. Dersom avtalen sies opp, vil Storebrand på grunn av muligheten for fremtidige erstatningskrav som kan tilbakeføres til avtaleforholdet, lagre opplysningene frem til foreldelsesfristen for de aktuelle produktene er utløpt. Opplysningene kan likevel behandles til annet formål så fremt det foreligger selvstendig lovgrunnlag eller etter personopplysningsloven § 8.

Opplysninger som vi etter lov er pålagt å oppbevare lenger vil ikke bli slettet etter ovennevnte frister.

Om du lurer på noe rundt Storebrands behandling av personopplysninger kan du kontakte vårt kunde- og personvernombud på e-post kundeombudet@storebrand.no.

Behandlingsansvarlig

Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. I Storebrandkonsernet er behandlingsansvarlig det selskapet som er avtalepart mot kunden.

Databehandler er den som behandler data på vegne av den behandlingsansvarlige, for eksempel våre underleverandører.

Cookies og analyseverktøy

I Storebrand brukes cookies på nettsidene for at besøksstatistikken vår skal være pålitelig og for å øke funksjonaliteten på våre sider. I enkelte tilfeller vil vi kunne bruke cookies også i forbindelse med markedsføring av våre produkter og tjenester. En cookie er en liten tekstfil som blir lagret på din harddisk av sidene du besøker.

Storebrand benytter analyseverktøyene Webtrends og i noen tilfeller Google Analytics for å samle inn informasjon om antall besøk på våre nettsider, hvilke sider som blir besøkt og lignende. Vi bruker denne informasjonen til å analysere bruken av våre nettsider og for å forbedre kvaliteten på sidene. Informasjonen inneholder ikke identifiserbare personlige opplysninger.

For brukere som ikke ønsker å dele denne type anonyme data med Storebrand kan lenkene under benyttes.

[Bruk denne lenken for å reservere deg mot Google Analytics sin bruk av anonyme data](#)

Ansvar ved feil, mangler og tilgjengelighet

Storebrand anser informasjonen på sine internettsider som pålitelig, men kan likevel ikke garantere at informasjonen til enhver tid er korrekt, fullstendig eller tilgjengelig. Storebrand fraskriver seg således ethvert ansvar for feil, mangler og manglende tilgjengelighet på sidene. Det understrekes at sidene og all informasjon på sidene utelukkende retter seg mot brukere i Norge, med mindre annet uttrykkelig fremgår.

Immaterialrett

Storebrand har alle immaterielle rettigheter til nettsidene. Uautorisert bruk av sidene eller innholdet på disse er ikke tillatt.

Lenker

Storebrand påtar seg ikke noe ansvar for det materiale som er utarbeidet eller publiseres av tredjepart selv om sidene våre inneholder lenker til slike sider. Tredjeparten har selv ansvaret for at publisering på sine nettsider er i overensstemmelse med lover og regler. Storebrand fraskriver seg således ethvert ansvar for feil, mangler og manglende tilgjengelighet på sidene.



Startside No Privat Bedrift Om If

Om nettstedet

Om nettstedet

Bruk av cookies og elektroniske spor

Vi lagrer data om bruk av våre nettsider. Dels lagres data i informasjonskapsler (cookies) på din datamaskin, og dels lagrer vi elektroniske spor på if.no. Dette gjør vi dels for å måle trafikken på våre sider, og dels for å kunne tilpasse opplevelsen til hver enkelt besøk.

Hvilke opplysninger innhentes

Vi innhenter opplysninger om maskinvare og programvare på datamaskinen din, herunder IP-adresse, nettleser og operativsystem, domenenavn, tilgangstider og tilknyttede nettsideadresser. Disse opplysningene er nødvendige for å analysere bruken av ressursene våre, feilsøke på problemer, avverge svindel og forbedre tjenestene.

Vi innhenter også opplysninger om hvordan du og andre besøkere bruker nettsidene våre. Dette gjør vi for å forstå hva som fungerer bra og hva som fungerer mindre bra. Vi innhenter blant annet informasjon om hvilke sider du besøker og hvilke tjenester du bruker, og hvordan du brukere disse. Ved å samle informasjon fra mange besøkere finner vi mønstre i bruken av våre nettsider som kan vise oss hvor det er behov for forbedringer. Denne informasjonen blir brukt som grunnlag for videreutvikling av våre nettsider og netjtjenester.

Dersom du er kunde hos oss kan innhold, tilbud og tjenester tilpasses til deg basert på hva du har gjort og hvilke sider du har sett på ved tidligere besøk. Det kan også hende at en av våre kunderådgivere kontakter deg med tilbud hvis du avbryter et kjøp i nettbutikken.

Ved å bruke nettsidene til If Skadeforsikring NUF (if.no) samtykker du til at vi, så fremt gjeldende lov tillater det, kan bruke opplysninger om din bruk av våre sider på følgende måte:

- lagre informasjon om hvordan du bruker nettsidene, for eksempel hvor ofte du besøker nettsidene, hvilke sider du besøker, og hvilke tjenester du bruker på sidene,
- tilpasse nettsidene og informasjonen til deg basert på informasjon vi har lagret
- kontakte deg som allerede er kunde i If med tilbud og informasjon om andre produkter eller tjenester, hvis du ikke har reservert deg mot markedsføring i Brønnøysundregistrene eller hos If. Vi sletter personopplysningene for dette formål senest innen 14 dager.
- lage interne rapporter om bruken av nettsidene og bruke disse til videreutvikling.

Deaktivering av cookies

Nettlesere kan stilles inn slik at du automatisk nekter cookies eller blir informert om at en nettside inneholder cookies. Dette innebærer at visse funksjoner på vår hjemmeside ikke kan brukes.

Som beskrevet brukes også andre måter enn cookies for å innhente opplysninger.

© If Skadeforsikring NUF [Behandling av personopplysninger](#) [Cookies](#) [Sidekart](#) [Tilbass](#)

[If skadeforsikring SE](#) [If Skadeforsikring DK](#) [If Vahinkovakuutusyhtiö FI](#)